

# **EXHIBIT A**

This case has been designated as an eFiling case, for more information please visit [www.oakgov.com/efiling](http://www.oakgov.com/efiling).

**STATE OF MICHIGAN**

**IN THE CIRCUIT COURT FOR THE COUNTY OF OAKLAND**

BASHA DIAGNOSTICS, P.C. a Michigan  
Professional Corporation,

Plaintiff,

v

CHANGE HEALTHCARE TECHNOLOGY  
ENABLED SERVICES, LLC a Georgia Limited  
Liability Company, CHANGE HEALTHCARE,  
INC., a Delaware Corporation, OPTUM INC., a  
Delaware Corporation, UNITEDHEALTH  
GROUP, INC., a Delaware Corporation, and  
UNITEDHEALTHCARE, INC., a Delaware  
Corporation.

Defendants.

Case No. -CB  
2025-212987-CB  
Hon  
JUDGE VICTORIA  
VALENTINE

---

**BODMAN PLC**

Michelle Thurber Czapski (P47267)  
Erica J. Sarver (P80106)  
Nashara A.L. Peart (P83078)  
201 W. Big Beaver Road, Suite 500  
Troy, Michigan 48084  
(248) 743-6000  
[mczapski@bodmanlaw.com](mailto:mczapski@bodmanlaw.com)  
[esarver@bodmanlaw.com](mailto:esarver@bodmanlaw.com)  
[npeart@bodmanlaw.com](mailto:npeart@bodmanlaw.com)  
*Attorneys for Plaintiff*

---

**COMPLAINT**

There is no other pending or resolved  
civil action arising out of the transaction  
or occurrence alleged in this complaint.

Further, this case involves a business or commercial  
dispute under MCL 600.8031 and thus meets  
the statutory requirements to be  
assigned to the Business Court Docket.

Plaintiff Basha Diagnostics, P.C. (“Basha”), by and through its attorneys, Bodman PLC, brings this Complaint against Defendants Change Healthcare Technology Enabled Services, LLC (“Change”), Change Healthcare, Inc. (“Change Healthcare”), Optum, Inc., (“Optum”), UnitedHealth Group, Inc., (“UHG”) and UnitedHealthcare, Inc. (“UHC”), and in support thereof states as follows:

### **NATURE OF THE ACTION**

1. UHG is one of the largest health insurers in the United States and is the parent company of defendants UHC and Optum.

2. Defendant Change Healthcare is a healthcare technology company created in 2017 after the merger of Change Healthcare Holdings, Inc. and McKesson Technology Solutions.<sup>1</sup> It is owned by Defendants UHG and Optum.

3. Defendant Change, formerly known as PST Services, LLC, is a wholly-owned subsidiary of Change Healthcare that offers, among other things, patient platforms to review and access medical reports, as well as medical billing and coding services.

4. Basha and Change, via an amended Masters Services Agreement effective October 1, 2016 (the “Agreement”), agreed that Change would provide practice management services related to Basha’s radiology care, and web-based reporting and billing services. Change also agreed to provide Basha with 24-hour access to a client reporting portal to bill insurance companies for patient care, and to receive payments therefrom.

---

<sup>1</sup> *McKesson and Change Healthcare Complete the Creation of New Healthcare Information Technology Company* (March 2, 2017) <https://www.mckesson.com/about-mckesson/newsroom/press-releases/2017/mckesson-and-change-healthcare-complete-the-creation-of-new-healthcare-information-technology-company/> (last visited February 19, 2025).

5. The parties performed under the Agreement until February 21, 2024, when Change Healthcare became the target of a serious ransomware cyber incident that resulted in a massive data breach (the “Data Breach”). The Data Breach led to a leak of unprecedented amounts of patient Protected Health Information (“PHI”).

6. Defendants’ immediate response to the Data Breach took critical systems offline, with little to no explanation given to Basha about its sudden inability to service its clients. Basha required these systems to properly deliver patient care and to submit billing to patients and various insurers.

7. The Agreement required Change to safeguard Basha’s patient information. The Data Breach constituted a breach of the Agreement. Aside from the contractual implications, the Data Breach resulted in a breach of Defendants’ duty to meet statutory requirements for the maintenance of PHI as required by the Health Insurance Portability and Accountability Act of 1996 (“HIPPA”).

8. Defendants have since failed to properly address the Data Breach, leaving Basha unable to access critical data necessary for operations, most importantly rendering Basha unable to process payments and other claims. To date, Basha continues to be impacted in its ability to initiate, process, or receive proceeds of insurance claims and other payments from its patients and their insurers.

9. Basha has paid, and continues to pay, significant fees for these services. Change Healthcare, UHG, UHC, and Optum have been unjustly enriched because Basha’s access to patient and medical billing platforms remains significantly hampered, crippling Basha’s ability to serve its clients.

10. Basha seeks damages against Defendants for their respective breach of contract, negligence, and resultant unjust enrichment.

### **PARTIES**

11. Plaintiff incorporates all preceding paragraphs as if fully set forth herein.

12. Plaintiff Basha is a Michigan professional corporation with its principal place of business in Royal Oak, Michigan.

13. Defendant Change is a Georgia limited liability company that does business in Oakland County, Michigan.

14. Defendant Change Healthcare is a Delaware corporation that does business in Oakland County, Michigan.

15. Defendant UHG is a Delaware corporation that does business in Oakland County, Michigan.

16. Defendant UHC is a Delaware corporation that does business in Oakland County, Michigan.

17. Defendant Optum is a Delaware corporation that does business in Oakland County, Michigan.

### **JURISDICTION AND VENUE**

18. Plaintiff incorporates all preceding paragraphs as if fully set forth herein.

19. This Court has personal jurisdiction over Change because of its and Basha's agreement that any disputes related to the Agreement will be heard in a court of competent jurisdiction in Oakland County, Michigan. MCL 600.711(2).

20. This court has personal jurisdiction over Change Healthcare, UHG, UHC, and Optum because they conduct business in Oakland County, Michigan. MCL 600.711(3).

21. This Court also has subject matter jurisdiction over this matter because the amount in controversy exceeds \$25,000.

22. Venue is proper in this Court because defendants conduct business in Oakland County, Michigan. MCL 600.1621(a).

### **FACTUAL ALLEGATIONS**

#### **The Agreement and Defendants' Statutory Duties**

23. Plaintiff incorporates all preceding paragraphs as if fully set forth herein.

24. Effective October 1, 2016, Basha and PST Services, Inc. ("PST") entered into the Agreement, whereby PST agreed to provide Basha with practice management services related to radiology care, including access to patient record review and editing, and medical coding and billing services. These services include the submission of medical billing to patients and relevant insurance carriers. A copy of the Agreement is attached hereto as **Exhibit 1**.

25. As announced on March 2, 2017, PST's parent company and McKesson Technology Solutions combined to create Change Healthcare. As a part of the merger, PST's name was changed to Change Healthcare Technology Enabled Services, LLC. This change impacted the Agreement only to change the party name, but did not impact the terms or conditions of the Agreement already in effect.

26. The Agreement set forth several requirements for Change's delivery of services to Basha, many based on duties as ascribed by HIPAA, including how PHI is to be used and protected, among other things. Relevant sections of the Agreement include:

- §2.1.2      Responsibilities. Service Provider agrees to perform the Services in accordance with all material applicable laws, rules and regulations...
- §4.1.1      Use and Disclosure of Confidential Information. ...Except as expressly permitted in this MA, neither party will: (i) disclose the other party's confidential information except (a) to its employees or contractors who have a need to know and are bound by confidentiality

terms no less restrictive than those contained in this MA, or (b) to the extent required by law following prompt notice of such obligation to the other party...Each party will use all reasonable care in handling and securing the other party's confidential information and will employ all security measures used for its own proprietary information of similar nature.

§4.7.1(c)(i) Other Warranties. Service Provider represents and warrants that it will perform all of its obligations under the Agreement in a timely, professional and workmanlike manner, in accordance with all of the terms of the MA and the applicable Service Schedules.

§2.1 of Exhibit A – Business Associate Addendum Uses and Disclosures of PHI Pursuant to the Underlying Agreement. Except as otherwise limited in this Addendum, Business Associate may use or disclose PHI only to perform functions, activities or services for, or on behalf of, Customer as specified in the Underlying Agreement or as Required by Law, provided that such use or disclosure would not violate the Privacy Rule if done by Customer.<sup>2</sup>

§3.1 of Exhibit A – Business Associate Addendum Appropriate Safeguards. Business Associate will use appropriate safeguards and will, after the compliance date of the HIPAA Final Rule<sup>3</sup>, comply with the Security Rule<sup>4</sup> with respect to Electronic PHI to prevent use or disclosure of such information other than as provided for by the Underlying Agreement and this Addendum.

§3.2 of Exhibit A – Business Associate Addendum Reporting of Improper Use of Disclosure, Security Incident or Breach. Business Associate will report to Customer any use or disclosure of PHI not permitted under this Addendum, Breach of Unsecured PHI or any Security Incident, without unreasonable delay...

§3.13 of Exhibit A – Business Associate Addendum HIPAA Final Rule Applicability....Business Associate agrees, as of the compliance date of the HIPAA Final Rule, to comply with applicable requirements imposed under the HIPAA Final Rule, including any amendments thereto.

---

<sup>2</sup> The HIPAA "Privacy Rule" means the Standards for Privacy of Individually Identifiable Health Information, part of HIPAA, and found at 45 CFR Part 160 and Part 164, Subparts A and E.

<sup>3</sup> The "Final Rule" means the Final Omnibus Rule issued on January 25, 2013 by the Office of Civil Rights of the U.S. Department of Health and Human Services, implementing changes to, among other things, the Privacy Rule, Security Rule and Breach Notification Rule.

<sup>4</sup> The HIPAA "Security Rule" means the Security Standards at 45 CFR Part 160 and Part 164, Subparts A and C.

Schedule 1, §2.2.1(c)      Service Provider Responsibilities. Service Provider will [p]repare and submit claims to insurance carriers or to patients directly if no insurance information was provided within twenty four (24) hours after receipt of all information necessary to submit claims.

Schedule 2, §2.1.1(a)(i)      Service Provider Responsibilities. Basic User Access. [Change will] [p]rovide 24 hour access, less scheduled or unscheduled downtime for maintenance or repair, from any Internet access point to the Client reporting portal...

27. Although not a signatory to the Agreement, Change Healthcare, UHG, UHC, and Optum also have statutory duties under HIPAA that they must adhere to as corporations that handle PHI. The HIPPA Privacy Rule, the Final Rule, and the HIPPA Security Rule are equally applicable to Defendants, and Basha relied on Defendants to carry out their statutory duties to safeguard patient information.

28. Defendants' failure to safeguard information allowed for the Data Breach to occur. The Data Breach was the cause of Basha's critical systems being taken offline, and the cause of Basha being unable to access systems designed for it to both bill and receive payment from various insurance carriers, and to bill patients directly.

### **The Data Breach**

29. Plaintiff incorporates all preceding paragraphs as if fully set forth herein.

30. Because of Defendants' failures to perform their statutorily required duties under HIPAA, on February 21, 2024, a hacker group called Blackcat, also known as ALPHV or Noverus, launched a ransomware heist against Change Healthcare, affecting all of its subsidiaries, including Change. Various reports related to the Data Breach are attached hereto as **Exhibit 2**.

31. According to reports, disruptions in Change Healthcare's services continued long after the Data Breach was reported and caused a leak of over six terabytes of highly sensitive medical and dental records and other PHI.



32. On a webpage that Change Healthcare dedicated to documenting updates to the public following the Data Breach, Change Healthcare did not identify issues related to the Data Breach as “resolved” until May 7, 2024, some *two and a half months later*. A copy of Change Healthcare’s list of updates can be found at **Exhibit 3**. But the Data Breach was very far from resolved in May 2024. Basha was not able to begin submitting claims again until mid to late August 2024, some *six months* after the Data Breach occurred. And even then, Defendants’ systems were not, and still are not, fully operational.

33. Change’s breach of the Agreement, and Defendants’ failure to meet their statutorily required duties to protect patient PHI caused significant damages to Basha as it struggled to provide efficient client service, being unable to access client records, or bill patients and insurance carriers.

34. What further underscores Defendants’ blatant failure to undertake their duties is the fact that the Data Breach was preventable. Defendants’ cybersecurity practices fell very short of the requirements set forth by HIPAA – requirements that Defendants had a duty to meet.

35. In fact, the risk of a cyber security attack aimed at the healthcare sector was so prevalent that, on October 28, 2020, the Federal Bureau of Investigation (“FBI”), Cybersecurity and Infrastructure Security Agency (“CISA”), and the Department of Health and Human Services authored a joint cybersecurity advisory, including a comprehensive list of “Mitigations”, warning of the dangers of an “increased and imminent cybercrime threat to U.S. hospitals and healthcare providers.” (the “2020 Advisory”). A copy of the 2020 Advisory is attached hereto as **Exhibit 4**.

36. The threat of ransomware attacks on hospitals and healthcare providers remained prevalent, so much so that on December 18, 2023, the American Hospital Association published an article alerting the public to the release of another joint cybersecurity advisory by the FBI, CISA

and the Australian Signals Directorate's Australian Cyber Security Centre about the heightened risk of ransomware attacks (the "2023 Advisory"). The 2023 Advisory included yet another list of comprehensive "Mitigations". A copy of the 2023 Advisory is attached hereto as **Exhibit 5**.

37. Despite the readily available nature of these serious warnings and suggested mitigations, Defendants failed to secure patient PHI, leaving themselves open to a ransomware attack that sent shockwaves through the American healthcare sector and caused significant damage to Basha.

**Failure to Properly Address the Data Breach and Ongoing Repercussions**

38. For months following the Data Breach, Basha remained unable to fully access patient records, and lacked full access to the system used to bill patients and insurance carriers.

39. Basha set forth its ongoing issues in a demand for resolution dated December 19, 2024 (the "Demand"). A copy of the Demand is attached hereto as **Exhibit 6**.

40. In the Demand, Basha stated its belief that Change Healthcare failed to prevent the Data Breach, and that it also failed to properly respond to it. Change also failed to timely notify Basha of the Data Breach, and failed to offer adequate support to answer patient questions.

41. At the time of the Demand, Basha estimated its damages to be in excess of \$8,000,000, but stated that those damages remain unclear because of the ongoing delays with Defendants' provision of services to Basha.

42. Defendants' unpreparedness and failure to prevent the Data Breach was further exacerbated by their ineffective response to it. Change's breach of the Agreement has caused significant damage to Basha. Change Healthcare, UHC, UHG, and Optum have, and continue to be, unjustly enriched by Basha's continued payment for services that those Defendants are not providing, and Defendants have breached their statutorily required duties to Basha.

**CAUSES OF ACTION**

**COUNT I – BREACH OF CONTRACT**

**-Against Change-**

43. Plaintiff incorporates all preceding paragraphs as if fully set forth herein.

44. Basha and Change entered the Agreement, as amended, effective October 1, 2016.

45. The Agreement fully sets forth Change's obligations to Basha, including the obligation to safeguard PHI (see §3.1 of Exhibit A to the Agreement), timely notify Basha of any breach thereto (see §3.2 of Exhibit A to the Agreement), and to guarantee 24-hour access to the client reporting portal (see Schedule 2, §2.1.1(a)(i) of the Agreement).

46. When the Data Breach occurred, it resulted in a total interruption of services to Basha, stripping Basha of all the benefits conferred to it under the Agreement.

47. Basha was unable to begin submitting claims for payment until mid to late August 2024, some six months after the Data Breach occurred, resulting in a significant reduction in funds collected.

48. The Data Breach demonstrated that Change had breached its duty to erect appropriate safeguards around patient PHI as required by §3.1 of Exhibit A to the Agreement.

49. The Data Breach, and Change's response thereto, also resulted in breaches to several other sections of the Agreement, a non-exhaustive list of same being set forth in Paragraph 26 above.

50. Change's multiple breaches of the Agreement has caused damages to Basha estimated to be in excess of \$8,000,000.

**COUNT II – UNJUST ENRICHMENT**  
**-Against Change Healthcare, UHG, UHC, and Optum-**

51. Plaintiff incorporates all preceding paragraphs as if fully set forth herein.

52. Change Healthcare, UHG, UHC, and Optum failed to protect patient PHI, which would have safeguarded Basha from the damages it has incurred.

53. Since the Data Breach, Basha has and continues to pay Change Healthcare, UHG, UHC, and Optum, through their affiliate Change, for the services Change should be but is not providing.

54. Because Change Healthcare, UHG, UHC, and Optum continue to receive payment from Basha for services that are not being provided, Change Healthcare, UHG, UHC, and Optum continue to be in receipt of a benefit from Basha.

55. These continued payments result in an inequity to Basha because Change Healthcare, UHG, UHC, and Optum are retaining a benefit received from Basha without providing the services Basha is entitled to.

**COUNT III – NEGLIGENCE**  
**-Against All Defendants-**

56. Plaintiff incorporates all preceding paragraphs as if fully set forth herein.

57. Pursuant to HIPAA's Privacy Rule, the Final Rule, HIPPA's Security Rule and other applicable statutes, Defendants had a duty to protect patient PHI from attackers such as Blackcat.

58. Guidance from the FBI and CISA specifically related to the danger of ransomware attacks for healthcare organizations, also created a duty for Defendants to vigilantly protect patient PHI.

59. Defendants breached their duty by failing to ensure patient information was properly protected from attack, and by failing to quickly mitigate the results of the Data Breach, effects of which are still being felt by Basha today.

60. Defendants' breach of their duties is the cause of Basha's extensive damages, and namely its inability to bill insurers and receive payments therefrom.

61. Basha's damages are extensive, and remain ongoing, as full functionality of Change's services have not yet been restored.

**COUNT IV – TORTIOUS INTERFERENCE WITH BUSINESS EXPECTANCY**  
**-Against All Defendants-**

62. Plaintiff reincorporates all preceding paragraphs as if fully set forth herein.

63. Basha relied on Defendants to provide care to thousands of patients, and to meet its billing obligations with multiple insurers on behalf of its patients.

64. Defendants, who are among the leading providers of medical technology and online platforms to facilitate patient care and medical billing, know or should have known that Basha was relying on them to meet its business obligations to multiple other parties.

65. Defendants knew or should have known that Basha's patients' health insurance contracts impose strict timing requirements for the submission of claims for payment.

66. Defendants have intentionally delayed the restoration of their services, and have failed to fully resume their services to date, even though nearly a year has passed since the Data Breach.

67. Defendants have also intentionally failed to handle the Data Breach in a reasonable manner, negatively impacting patients' and other third-parties' trust in Basha to meet their various needs and contractual obligations. Patients have received incorrect account statements and have

been regularly hung up on by Optum staff when trying to call in for help. See Exhibit 6. This severely undermines Basha's business relationships with third parties.

68. Several of Basha's patients have had their claims rejected by their insurance companies because they were not timely submitted.

69. Defendants' interference has caused serious damage, not only to Basha's reputation and relationships with its patients, but also economically as Basha cannot consistently meet insurance timing requirements for issuing bills, resulting in significant lost collectables for Basha.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff respectfully requests that this Court enter judgment in its favor on all counts, including the following specific relief:

- a. For an award of damages in an amount in excess of \$25,000, the exact amount to be determined by the trier of fact;
- b. For an award of attorney's fees, costs, and litigation expenses as allowed by law; and
- c. For all other relief that this Court deems appropriate.

Respectfully submitted,

/s/ Michelle Thurber Czapski  
Michelle Thurber Czapski (P47267)  
Erica J. Sarver (P80106)  
Nashara A.L. Peart (P83078)  
BODMAN PLC  
201 W. Big Beaver Road, Suite 500  
Troy, Michigan 48084  
(248) 743-6000  
mczapski@bodmanlaw.com  
esarver@bodmanlaw.com  
npeart@bodmanlaw.com  
*Attorneys for Plaintiff*

Dated: February 20, 2025.

**JURY DEMAND**

Plaintiff Basha Diagnostics, P.C. through its attorneys Bodman PLC, hereby demands a trial by jury in the above-captioned matter.

Respectfully submitted,

/s/ Michelle Thurber Czapski  
Michelle Thurber Czapski (P47267)  
Erica J. Sarver (P80106)  
Nashara A.L. Peart (P83078)  
BODMAN PLC  
201 W. Big Beaver Road, Suite 500  
Troy, Michigan 48084  
(248) 743-6000  
mzczapski@bodmanlaw.com  
esarver@bodmanlaw.com  
npeart@bodmanlaw.com  
*Attorneys for Plaintiff*

Dated: February 20, 2025.

# ***EXHIBIT 1***



# CHANGE

## HEALTHCARE

Dear Valued Customer,

As originally announced in the press release dated March 2, 2017, our parent company and McKesson Technology Solutions combined to create a new healthcare information technology company. The new company is named Change Healthcare and is focused on delivering financial, operational and clinical benefits to the healthcare marketplace. As a wholly-owned subsidiary of Change Healthcare, PST Services, LLC will align itself with the new company by rebranding as Change Healthcare. In keeping with our commitment to transparency expressed in that press release, we want to share important information that may affect your payment and financial reporting processes in calendar year 2018.

This rebranding process will result in the following name changes:

OLD Contracting Entity Name	NEW Contracting Entity Name
PST Services, LLC	Change Healthcare Technology Enabled Services, LLC

These changes DO NOT impact the terms or conditions of any contracts that are currently in effect with the old contracting entities. Moreover, existing contracts do not require any immediate changes to the contracting name. Contracts that are renewed or renegotiated in the future will utilize the applicable new entity name and will be modified appropriately to reflect such name change.

The previous payee/remit to name was typically **PST Services, LLC**. This will need to be modified to **Change Healthcare** to reflect our new contracting entity name (effective January 1, 2018).

The remittance address for the above entities has not changed and remains:

PO Box 742526; Atlanta, GA 30374-2526

The rebranding will also impact the W-9 we need to provide you pursuant to IRS guidelines. We will be providing you a new W-9 for your records that reflects the new name of the company once the name change is effective. Your organization will need this information when creating your 1099-MISC form(s) for the IRS.

We trust this information will help you understand the slight differences that will appear on your invoices beginning with the January 2018 invoicing statement. However, in the event you may have additional questions, please contact the Client Manager listed on your invoices.

On behalf of the 15,000 persons of the new Change Healthcare, we thank you for your partnership as we work together to inspire a better healthcare system. Thanks again for your attention to the above information.

<b>Form W-9</b> (Rev. November 2017) Department of the Treasury Internal Revenue Service	<b>Request for Taxpayer Identification Number and Certification</b> ▶ Go to <a href="http://www.irs.gov/FormW9">www.irs.gov/FormW9</a> for instructions and the latest information.	Give Form to the requester. Do not send to the IRS.
---	--	---

1 Name (as shown on your income tax return). Name is required on this line; do not leave this line blank.

**Change Healthcare LLC**

2 Business name/disregarded entity name, if different from above

**Change Healthcare Technology Enabled Services LLC (FEIN: 58-1853146)**

3 Check appropriate box for federal tax classification of the person whose name is entered on line 1. Check only one of the following seven boxes.

☐ Individual/sole proprietor or single-member LLC

☐ C Corporation

☐ S Corporation

☐ Partnership

☐ Trust/estate

☒ Limited liability company. Enter the tax classification (C=C corporation, S=S corporation, P=Partnership) ▶ **P**

Note: Check the appropriate box in the line above for the tax classification of the single-member owner. Do not check LLC if the LLC is classified as a single-member LLC that is disregarded from the owner unless the owner of the LLC is another LLC that is not disregarded from the owner for U.S. federal tax purposes. Otherwise, a single-member LLC that is disregarded from the owner should check the appropriate box for the tax classification of its owner.

☐ Other (see instructions) ▶

4 Exemptions (codes apply only to certain entities, not individuals; see instructions on page 3):

Exempt payee code (if any) \_\_\_\_\_

Exemption from FATCA reporting code (if any) \_\_\_\_\_

(Applies to accounts maintained outside the U.S.)

5 Address (number, street, and apt. or suite no.) See instructions.

**5995 Windward Parkway**

6 City, state, and ZIP code

**Alpharetta, GA 30005**

7 List account number(s) here (optional)

**Part I Taxpayer Identification Number (TIN)**

Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN*, later.

Note: If the account is in more than one name, see the instructions for line 1. Also see *What Name and Number To Give the Requester* for guidelines on whose number to enter.

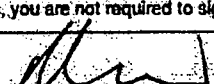
Social security number									
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]				
OR									
Employer identification number									
8	1	-	3	6	1	1	5	6	0

**Part II Certification**

Under penalties of perjury, I certify that:

- The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
- I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
- I am a U.S. citizen or other U.S. person (defined below); and
- The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

**Certification instructions.** You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.

**Sign Here**      Signature of U.S. person ▶       Date ▶ **12/22/2017**

## General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

**Future developments.** For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to [www.irs.gov/FormW9](http://www.irs.gov/FormW9).

## Purpose of Form

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS must obtain your correct taxpayer identification number (TIN) which may be your social security number (SSN), individual taxpayer identification number (ITIN), adoption taxpayer identification number (ATIN), or employer identification number (EIN), to report on an information return the amount paid to you, or other amount reportable on an information return. Examples of information returns include, but are not limited to, the following:

- Form 1099-INT (interest earned or paid)

- Form 1099-DIV (dividends, including those from stocks or mutual funds)
- Form 1099-MISC (various types of income, prizes, awards, or gross proceeds)
- Form 1099-B (stock or mutual fund sales and certain other transactions by brokers)
- Form 1099-S (proceeds from real estate transactions)
- Form 1099-K (merchant card and third party network transactions)
- Form 1098 (home mortgage interest); 1098-E (student loan interest); 1098-T (tuition)
- Form 1099-C (canceled debt)
- Form 1099-A (acquisition or abandonment of secured property)

Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN.

If you do not return Form W-9 to the requester with a TIN, you might be subject to backup withholding. See *What Is Backup Withholding*, later.

**CONFIDENTIAL AND PROPRIETARY**Client: Basha Diagnostics, P.C.  
Amendment Number: P201610010724**AMENDMENT**

This Amendment (this "Amendment") amends the Master Services Agreement (RMS153968) that became effective on June 14, 2016 (the "MA") between Basha Diagnostics, P.C. ("Client") and PST Services, Inc. ("Service Provider") and is effective the latest date in the signature block below.

For good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. Service Schedule 1 (Scope of Services - Radiology). Section 1.1 (Initial Term of Schedule). The MA is amended by changing the Commencement Date listed in Section 1.1 of Service Schedule 1 to October 1, 2016.
2. Service Schedule 1 (Scope of Services Radiology). Section 2.2.1 (Service Provider Responsibilities). The MA is amended by deleting Section 2.2.1(l) of Service Schedule 1 in its entirety and inserting the following in lieu thereof:

2.2.1(l) Notify Client in writing of the Monthly Refund Amount owed by Client for the previous month. Upon Client's deposit of the Monthly Refund Amount in the Refund Account, prepare and send the applicable individual patient and carrier refund checks to Client for signature by Client.

3. Service Schedule 1 (Scope of Services Radiology). Section 2.2.2 (Client Responsibilities). The MA is amended by deleting Section 2.2.2(k) of Service Schedule 1 in its entirety and inserting the following in lieu thereof:

2.2.2(k) Maintain and fund a separate bank account for refunds due by Client (the "Refund Account"). Fund such Refund Account each month in an amount equal to the total refund payments due by Client to individual patients and/or carriers (the "Monthly Refund Amount") within ten business days of Client's receipt of notification from Service Provider of such Monthly Refund Amount owed by Client. Client further authorizes Service Provider, upon Client's deposit of the Monthly Refund Amount in the Refund Account, to prepare the applicable refund checks and send refund checks to Client for signature. Client will sign and mail refund checks within 30 days of Client's receipt of prepared refund checks from Service Provider.

4. This Amendment may be executed in multiple counterparts, each of which shall be deemed an original and all of which together shall be deemed one and the same instrument.
5. Capitalized terms used herein and not otherwise defined have the same meaning as in the MA. In the event any term or condition of this Amendment is inconsistent with any term or condition of the MA, the terms of this Amendment will control. Except as stated above, all terms of the MA shall remain in full force and effect. Service Provider and Client represent and warrant that they have the full power and authority to enter into this Amendment, that there are no restrictions or limitations on their ability to perform under this Amendment, and that the person executing this Amendment has the full power and authority to do so.

IN WITNESS WHEREOF, and in agreement hereto, the parties have executed this Amendment on the dates set forth below.

Basha Diagnostics, P.C.

By: [Signature]Print Name: YAHYA MOSSA BASHATitle: PRESIDENTDate: 8/31/16

PST Services, Inc.

By: [Signature]Print Name: Christopher W. RobertsonTitle: Senior VP, OperationsDate: 9.2.16

CONFIDENTIAL AND PROPRIETARY

Client: Basha Diagnostics, P.C.  
Amendment Number: P201610010724AMENDMENT

This Amendment (this "Amendment") amends the Master Services Agreement (RMS153968) that became effective on June 14, 2016 (the "MA") between Basha Diagnostics, P.C. ("Client") and PST Services, Inc. ("Service Provider") and is effective the latest date in the signature block below.

For good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. Service Schedule 1 (Scope of Services – Radiology). Section 1.1 (Initial Term of Schedule). The MA is amended by changing the Commencement Date listed in Section 1.1 of Service Schedule 1 to October 1, 2016.
2. Service Schedule 1 (Scope of Services Radiology). Section 2.2.1 (Service Provider Responsibilities). The MA is amended by deleting Section 2.2.1(l) of Service Schedule 1 in its entirety and inserting the following in lieu thereof:

2.2.1(l) Notify Client in writing of the Monthly Refund Amount owed by Client for the previous month. Upon Client's deposit of the Monthly Refund Amount in the Refund Account, prepare and send the applicable individual patient and carrier refund checks to Client for signature by Client.

3. Service Schedule 1 (Scope of Services Radiology). Section 2.2.2 (Client Responsibilities). The MA is amended by deleting Section 2.2.2(k) of Service Schedule 1 in its entirety and inserting the following in lieu thereof:

2.2.2(k) Maintain and fund a separate bank account for refunds due by Client (the "Refund Account"). Fund such Refund Account each month in an amount equal to the total refund payments due by Client to individual patients and/or carriers (the "Monthly Refund Amount") within ten business days of Client's receipt of notification from Service Provider of such Monthly Refund Amount owed by Client. Client further authorizes Service Provider, upon Client's deposit of the Monthly Refund Amount in the Refund Account, to prepare the applicable refund checks and send refund checks to Client for signature. Client will sign and mail refund checks within 30 days of Client's receipt of prepared refund checks from Service Provider.

4. This Amendment may be executed in multiple counterparts, each of which shall be deemed an original and all of which together shall be deemed one and the same instrument.
5. Capitalized terms used herein and not otherwise defined have the same meaning as in the MA. In the event any term or condition of this Amendment is inconsistent with any term or condition of the MA, the terms of this Amendment will control. Except as stated above, all terms of the MA shall remain in full force and effect. Service Provider and Client represent and warrant that they have the full power and authority to enter into this Amendment, that there are no restrictions or limitations on their ability to perform under this Amendment, and that the person executing this Amendment has the full power and authority to do so.

IN WITNESS WHEREOF, and in agreement hereto, the parties have executed this Amendment on the dates set forth below.

Basha Diagnostics, P.C.

PST Services, Inc.

By: Yahya Mossa Basha

By: \_\_\_\_\_

Print Name: YAHYA MOSSA BASHA

Print Name: \_\_\_\_\_

Title: PRESIDENT

Title: \_\_\_\_\_

Date: 8/31/16

Date: \_\_\_\_\_

CONFIDENTIAL AND PROPRIETARY

Client: Basha Diagnostics  
Contract Number: RMS153968**MASTER SERVICES AGREEMENT**

This MASTER SERVICES AGREEMENT (this "MA") is effective the latest date in the signature block below (the "Effective Date") between PST Services, Inc. ("Service Provider") and Basha Diagnostics, P.C. ("Client"), consisting of the MA Terms and Conditions and all Exhibits, Schedules, and Amendments. This MA governs all the Services described on a Service Schedule that is included in this MA during the term.

Subject to the terms and conditions of this MA, Client agrees to purchase from Service Provider, and Service Provider agrees to provide Client with, the service(s) listed in the table below (individually, a "Service" and collectively, the "Services"). The description of each Service provided under this MA and any additional terms and conditions relating to such Service are set forth in the Service Schedule referenced in the table below and attached hereto.

Service Schedule	
Radiology	Service Schedule 1
McKesson Practice Focus Web Based Reporting	Service Schedule 2

This MA is executed by an authorized representative of each party.

**BASHA DIAGNOSTICS, P.C.**

By:

Printed Name:

Title:

Date:

Tax ID:

ABDUL BASHA  
MANAGER  
6/10/16  
28-2753824

**PST SERVICES, INC.**

By:

Printed Name:

Title:

Date:

Service Provider:  
 5995 Windward Parkway  
 Alpharetta, Georgia 30005  
 Attention: President

Client:  
 30701 Woodward Avenue  
 Royal Oak, Michigan 48073  
 Attention: \_\_\_\_\_

With a copy to the General Counsel at the same address

yes ☐  
 no ☐

invoices sent to above address

If no, list invoice address below:

\_\_\_\_\_  
 \_\_\_\_\_

Attention: \_\_\_\_\_



**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
Contract Number: RMS153968

**MA TERMS AND CONDITIONS**

**1. TERM**

- 1.1. This MA will begin on the Effective Date and continues until termination or expiration of each Service Schedule attached hereunder, unless earlier terminated as set forth herein.
- 1.2. Further, this MA will remain in force so long as there is an active Service Schedule(s).

**2. SERVICES**

**2.1. Responsibilities.**

- 2.1.1. Service Provider will perform the Services set forth on the applicable Service Schedule(s) on behalf of Client.
- 2.1.2. Service Provider agrees to perform the Services in accordance with all material applicable laws, rules and regulations, including applicable third-party payer policies and procedures.
- 2.1.3. Client will provide Service Provider with the necessary data in the proper format to enable Service Provider to properly furnish the Services and any information set forth in the Service Schedule(s) on a timely basis and in a format reasonably acceptable to Service Provider (the "Client Responsibilities"). Client authorizes, to the extent necessary, and directs Service Provider to release any or all necessary data and information (including, without limitation, "Individually Identifiable Health Information" as such term is defined in 45 C.F.R. § 160.103) received by Service Provider in the performance of the Services hereunder. Further, to the extent required by the applicable federal and state laws and regulations, including but not limited to, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and the Telephone Consumer Protection Act (47 U.S.C. Section 227) and related regulations, as well as similar state laws and regulations governing telephone communications with consumers, if any, Client shall obtain and maintain a record of all necessary authorizations and agreement from patients to allow the Service Provider to contact the patients by telephone as may be necessary in the performance of the Services and shall ensure that all information it provides to Service Provider may be used by Service Provider for telephone contacts (subject to the "minimum necessary" requirements of HIPAA).

**2.2. Operating Procedures.**

- 2.2.1. Client acknowledges (i) that the Services or obligations of Service Provider hereunder may be dependent on Client providing access to data, information, or assistance to Service Provider from time-to-time (collectively, "Cooperation"); and (ii) that such Cooperation may be essential to the performance of the Services by Service Provider. The parties agree that any delay or failure by Service Provider to provide the Services hereunder which is caused by Client's failure to provide timely Cooperation, as reasonably requested by Service Provider, shall not be deemed a breach of Service Provider's performance obligations under this MA. Therefore, Client hereby acknowledges that such variables are specifically excluded from Service Provider's liability under this MA.
- 2.2.2. Client acknowledges that Service Provider has every incentive to perform the Services in a timely and proficient manner, but the timing and amount of collections generated by the Services are subject to numerous variables beyond Service Provider's control including, without limitation, (i) the inability of third parties or systems to accurately process data, (ii) the transmission of inaccurate, incomplete or duplicate data to Service Provider, (iii) untimely reimbursements or payer bankruptcies, (iv) late charge documentation submissions by Client, or (v) managed care contract disputes between payers and Client. Therefore, Client hereby acknowledges that such variables are specifically excluded from Service Provider's liability under this MA.
- 2.2.3. Service Provider will be the sole provider of the Services to Client.

**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
Contract Number: RMS153968

**3. PAYMENT**

- 3.1. Lockbox. An electronic lockbox will be maintained in Client's name at a bank designated by Client. All cash receipts will be deposited into the lockbox. Service Provider will have no ownership rights in the lockbox and will have no right to negotiate or assert ownership of checks made payable to Client. Client will be responsible for all fees associated with such lockbox.
- 3.2. Invoicing Terms. Beginning on the Commencement Date (as defined in each Service Schedule), Client will pay all fees and other charges in U.S. dollars within 30 days after the invoice date. Prior to the Commencement Date, Client further agrees to establish an automatic electronic funds debit arrangement for paying Service Provider's invoices.
- 3.3. Late Payments. Intentionally Omitted.
- 3.4. Suspension of the Services. Service Provider reserves the right to suspend performance of the Services (i) for nonpayment of sums owed to Service Provider that are 30 days or more past due, where such breach is not cured within ten days after notice to Client, or (ii) if such suspension is necessary to comply with applicable law or order of any governmental authority.
- 3.5. Fee Change. Once every twelve months following the initial three (3) years after the Effective Date (if the MA has not been terminated prior to or at that time), either party may request a fee change in the event of a material change in legislation, Client's business or other market conditions which result in a material change in either the cost associated with Service Provider's provision of the Services or Service Provider's anticipated revenues under this MA. In addition, Service Provider may request a fee change in the event (i) Client fails to disclose to Service Provider information relating to Client's practice, which information, if disclosed prior to the Effective Date, would have led Service Provider to propose a higher fee or (ii) any of the information provided by Client to Service Provider upon which the practice assumptions set forth in any applicable Service Schedule are based, is or becomes inaccurate. In the event either party requests a change in the Fee, the requesting party will provide the non-requesting party with ninety (90) days' prior written notice (the "Notice Period") of the requested change (the "Notice") and such fee change will be effective at the end of the Notice Period. If the non-requesting party provides the requesting party written notice during any such Notice Period that any such fee change request is unacceptable to the non-requesting party, the Agreement will terminate at the end of the Notice Period and the Fee in place at that time will remain in effect until the end of the Workout Period, if any.

**4. GENERAL TERMS****4.1. Confidentiality and Proprietary Rights.**

- 4.1.1. Use and Disclosure of Confidential Information. Each party may disclose to the other party confidential information. Except as expressly permitted by this MA, neither party will: (i) disclose the other party's confidential information except (a) to its employees or contractors who have a need to know and are bound by confidentiality terms no less restrictive than those contained in this MA, or (b) to the extent required by law following prompt notice of such obligation to the other party, or (ii) use the other party's confidential information for any purpose other than performing its obligations under this MA. Client will not disclose nor cause its employees, agents and representatives to disclose to anyone Service Provider's business practices, trade secrets or Confidential Information, except as legally required. Each party will use all reasonable care in handling and securing the other party's confidential information and will employ all security measures used for its own proprietary information of similar nature. Notwithstanding the foregoing, Client agrees that Service Provider may de-identify Client information consistent with the Privacy Rule (as this term is defined in Exhibit A hereto) and use such de-identified information for statistical compilations or reports, research and for other purposes (the "Uses") so long as such Uses are in compliance with all applicable laws. Such Uses shall be the sole and exclusive property of Service Provider.

**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
Contract Number: RMS153968

**4.1.2. Use and Disclosure of Billing Software.**

- (a) Client agrees that the software Service Provider uses to perform the Services (the "Billing System") is proprietary and confidential and that Service Provider is the sole owner or licensee of the Billing System. All report formats and reports generated by the Billing System are produced and will be made available to Client for internal operational purposes only.
- (b) Client will not disclose or cause its employees, agents and representatives to disclose to anyone the Billing System or any information it receives about the Billing System, except as legally required.
- (c) Access to Software. If Service Provider grants Client or its employees or agents "read-only" or "direct access" to the Billing System or other software provided by Service Provider by any means, Client agrees to the End User Terms and Conditions set forth in Exhibit D to this MA.

**4.1.3. Period of Confidentiality.** The restrictions on use, disclosure and reproduction of confidential information set forth in Section 4.1, which are a "trade secret" (as that term is defined under applicable law) will be perpetual, and with respect to other confidential information such restrictions will remain in full force and effect during the term of this MA and perpetually following the termination of this MA for any reason. Following the termination of this MA for any reason, each party will, upon written request, return or destroy all of the other party's tangible confidential information in its possession and will promptly certify in writing to the other party that it has done so.

**4.1.4. Injunctive Relief.** The parties agree that the breach, or threatened breach, of any provision of this Section 4.1 may cause irreparable harm without adequate remedy at law. Upon any such breach or threatened breach, the breached party will be entitled to seek injunctive relief to prevent the other party from commencing or continuing any action constituting such breach, without having to post a bond or other security and without having to prove the inadequacy of other available remedies. Nothing in this Section 4.1.4 will limit any other remedy available to either party.

**4.1.5. Retained Rights.** Client's rights in the Services will be limited to those expressly granted in this MA. Service Provider and its suppliers reserve all intellectual property rights not expressly granted to Client. All changes, modifications, improvements or new modules made or developed with regard to the Services, whether or not (i) made or developed at Client's request, (ii) made or developed in cooperation with Client, or (iii) made or developed by Client, will be solely owned by Service Provider or its suppliers. Service Provider retains title to all material, originated or prepared for Client under this MA. Client is granted a license to use such materials in accordance with this MA. For purposes of clarification, all data used in the reports prepared by Service Provider in the performance of Services for Client, and all rights and interests therein, shall be the sole property of Client. The form of the reports, work product, including processes and templates used to prepare such reports shall be the sole property of Service Provider.

**4.2. Termination.**

**4.2.1. Termination for Default.** Either party may terminate this MA by providing 30 days prior written notice of termination to the other party, if the other party (i) materially breaches this MA and fails to remedy or commence reasonable efforts to remedy such breach within 15 days, and materially cure within 30 days, after receiving notice of the breach from the terminating party, (ii) materially breaches this MA in such a way that cannot be remedied, (iii) commences dissolution proceedings or (iv) ceases to operate in the ordinary course of business.

**4.2.2. Termination for Payment Default.** Service Provider may terminate this MA immediately if Client defaults on its payment obligations under this MA and such



**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
Contract Number: RMS153968

payment default is not cured within ten (10) business days of written notice from Service Provider.

**4.2.3. Termination by Service Provider.**

- (a) Service Provider may terminate this MA without incurring any liability to Client if Service Provider does not receive a completed implementation discovery packet, a form of which is attached hereto as Exhibit E (to the extent applicable and the Client has the information requested), within three months after the Commencement Date of a Service Schedule and, following the expiration of such a three month period, fails to cure same within ten (10) business days of receiving a written notice from Service Provider. In the event of such a termination, Client will pay Service Provider all reasonable expenses directly related to this MA that were incurred in good faith by the Service Provider prior to the termination date; or
- (b) If Service Provider uses third-party software to provide the Services, Client agrees to execute additional documents other than the MA, including but not limited to nondisclosure or proprietary material documentation that is reasonably required by Service Provider or any other third-party software licensor. If Client is unwilling to sign such additional documentation, Service Provider may terminate this MA 90 days after Service Provider presented the documentation to Client.

**4.2.4. Termination by Client.** Client may terminate this MA immediately if Service Provider fails to cure any breach of the "Business Associate Addendum" (set forth on Exhibit A to this MA) within 30 days of Service Providers receipt of written notice from Client specifying the breach or if a Business Associate Addendum is terminated for any reason.

**4.2.5. Termination Procedures – Service Provider Billing System.** In the event this MA or any Service Schedule is terminated or expires, Client will notify Service Provider in writing no later than ten business days prior to the expiration or termination of the Service Schedule of its choice of either the option set forth in sub-Section (a) below or the option set forth in sub-Section (b) below as a means of transferring its accounts receivable from Service Provider to another provider of billing services (except as otherwise set forth in sub-Section (c) below, in which case only the procedures set forth in sub-Section (b) will apply).

- (a) Workout Period. Upon the effective date of termination/expiration, Service Provider shall cease to enter new patient and charge data into the Billing System on behalf of Client, but will continue to perform the Services identified in the applicable Service Schedule at the then-current rates hereunder, for a period of 90 days with respect to all of Client's accounts receivable arising from charges rendered prior to the termination date (such period hereinafter referred to as the "Workout Period"). After the Workout Period, Service Provider will discontinue processing such accounts receivable, and after full payment of all fees owed (1) deliver to Client a final list of accounts receivable and (2) provide reasonable transitional services, as set forth on Exhibit C to this MA. After completion of the above, Service Provider will have no further obligations to Client, except as expressly set forth in this MA or the Business Associate Addendum. The parties agree that all applicable terms and conditions of this MA will be in full force and effect until the end of the Workout Period.
- (b) Fees. For Client's accounts receivable for which Service Provider receives a Fee based on a percentage of the Net Collections, Client shall pay Service Provider, on or before the effective date of termination/expiration, a one-time fee equal to the average monthly invoice for the six (6) months immediately preceding the effective date of such

**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
Contract Number: RMS153968

termination multiplied by one and one-half (1.5) (the "Services Rendered Fee"). With respect to Client's accounts receivable for which Service Provider receives a Fee based on a set dollar amount, no additional fees shall be owed to Service Provider as of the effective date of termination/expiration. Upon the effective date of termination/expiration of this MA or Service Schedule, Service Provider shall be immediately relieved of its obligation to provide any further Services on behalf of Client. After full payment of all fees owed, including but not limited to the Services Rendered Fee, Service Provider will deliver to Client a final list of accounts receivable and provide reasonable Transitional Services, as set forth on Exhibit C to this MA. After completion of the above, Service Provider will have no further obligations to Client, except as expressly set forth in this MA or the Business Associate Addendum. The Services Rendered Fee does not limit the rights and remedies Service Provider may have against Client arising out of any breach of this MA.

(c) Default Selection. Intentionally Omitted.

4.2.6. Survival of Provisions. Those provisions of this MA that, by their nature, are intended to survive termination or expiration of this MA will remain in full force and effect after the expiration or termination of this MA for any reason, including, without limitation, the following Sections of this MA: 3 (Payment), 4.1 (Confidentiality), 4.3 (Limitation of Liability), 4.4 (Internet Disclaimer), 4.5 (Civil Monetary Fine or Penalty, Indemnification), 4.6.3 (Books and Records), and 4.10 – 4.26 (Governing Law – Entire Agreement).

4.2.7. Client's Remedies. In the event of any breach of Service Provider's obligations under this MA or any Service Schedule and failure to cure in accordance with Section 4.2.1, Client shall be entitled to seek all remedies allowed under law and equity.

4.3. Limitation of Liability.

4.3.1. Total Damages. Except for Service Provider's obligations under Section 4.5, Service Provider's total cumulative liability in connection with, or related to this MA will be limited to, whichever is greater: (i) \$1,000,000, or (ii) the sum of fees paid by Client to Service Provider for itself and/or the affected Practice during the 36-month period preceding the date of the claim, or (ii) if a claim arises after the expiration or termination of this MA or any Service Schedule for any reason, then to the sum of fees paid by Client to Service Provider for itself and/or the affected Practice during the 36-month period preceding the date of expiration or termination, as applicable, whether based on breach of contract, warranty, tort, product liability or otherwise. Client's total cumulative liability in connection with, or related to this MA will be limited to the sum of fees paid by Client to Service Provider during the 12-month period preceding the date of the claim, as applicable, whether based on breach of contract, warranty, tort, product liability or otherwise. Neither Party will have any liability for the inability of third parties or systems beyond the control of that Party, except that Service Provider shall be liable for all acts, omissions, negligence and willful misconduct of all its agents and subcontractors. For the avoidance of doubt, there is no cap on Service Provider's liability in connection with its indemnification and other obligations under Section 4.5.

4.3.2. Exclusion of Damages. IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER PARTY UNDER, IN CONNECTION WITH, OR RELATED TO THIS MA FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOST PROFITS OR LOSS OF GOODWILL, WHETHER BASED ON BREACH OF CONTRACT, WARRANTY, TORT, PRODUCT LIABILITY, OR OTHERWISE, AND WHETHER OR NOT SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
Contract Number: RMS153968

4.3.3. Material Consideration. THE PARTIES ACKNOWLEDGE THAT THE FOREGOING LIMITATIONS ARE A MATERIAL CONDITION FOR THEIR ENTRY INTO THIS MA.

4.4. Internet Disclaimer. CERTAIN PRODUCTS AND SERVICES PROVIDED BY SERVICE PROVIDER UTILIZE THE INTERNET. SERVICE PROVIDER DOES NOT WARRANT THAT SUCH SERVICES WILL BE UNINTERRUPTED, ERROR-FREE, OR COMPLETELY SECURE. SERVICE PROVIDER DOES NOT AND CANNOT CONTROL THE FLOW OF DATA TO OR FROM SERVICE PROVIDER'S OR CLIENT'S NETWORK AND OTHER PORTIONS OF THE INTERNET. SUCH FLOW DEPENDS IN LARGE PART ON THE INTERNET SERVICES PROVIDED OR CONTROLLED BY THIRD PARTIES. ACTIONS OR INACTIONS OF SUCH THIRD PARTIES CAN IMPAIR OR DISRUPT CLIENT'S CONNECTIONS TO THE INTERNET (OR PORTIONS THEREOF). ACCORDINGLY, SERVICE PROVIDER DISCLAIMS ANY AND ALL LIABILITY RESULTING FROM OR RELATED TO THE ABOVE EVENTS, EXCEPT TO THE EXTENT CAUSED BY THE SERVICE PROVIDER.

4.5. Civil Monetary Fine or Penalty. Indemnification. Service Provider will pay any civil or monetary fine or penalty and interest (but not overpayments) assessed against Client by Medicare, Medicaid or other third-party health insurance provider or any federal or state agency to the extent arising out of Service Provider's or any of its affiliates or subcontractors negligence or willful misconduct in the performance of its obligations under this MA. Overpayments received by Client are the sole responsibility of Client.

Service Provider will defend, indemnify, and hold Client harmless from any costs, expenses, damages, claims, action or other proceeding brought against Client to the extent that it is based on a claim that arises out of or is related to (i) the use of any Services delivered under this MA infringes any U.S. copyright or U.S. patent, or (ii) the Service Provider Services incorporate any misappropriated trade secrets. Service Provider will pay costs and damages finally awarded against Client as a result thereof; provided, that Client (A) notifies Service Provider of the claim within ten business days (provided, however, that failure to give such notification shall not affect the indemnification provided hereunder except to the extent that the ability to defend such claim or action is actually prejudiced as a result of such failure), (B) provides Service Provider with all reasonably requested cooperation, information and assistance, and (C) gives Service Provider the authority to defend and settle the claim (provided, however, that the Client shall have the right to participate in the defense thereof and to employ counsel at its own expense and separate from the counsel employed by the Service Provider, it being understood that the Party assuming the defense shall control such defense).

4.6. Audits.

4.6.1. Internal Audit by Client. Client may use its own internal resources ("Internal Auditors") to perform audits of Service Provider's accuracy and correctness of the accounting and internal controls performed and maintained by Service Provider. Service Provider will provide the Internal Auditors with information that the Internal Auditor determines to be reasonably necessary to perform and complete the audit procedures. Client agrees that an audit conducted under this section will be conducted at such times and in a manner that avoids undue disruption of Service Provider's operations.

4.6.2. Third-Party Audit by Client. Client may engage, at its own expense, independent, external, third-party auditors ("Third-Party Auditors") to perform audits of Service Provider's accuracy and correctness of the accounting and internal control performed and maintained by Service Provider. If Client engages Third-Party Auditors, who perform, or are associated with a group who performs, billing and accounts receivable management services substantially similar to any of the Services identified on any Service Schedule to this MA, such Third-Party Auditors may not visit Service Provider's processing facility or audit the actual billing and collection process. Service Provider will provide the information that the Third-

**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
Contract Number: RMS153968

Party Auditors determine to be reasonably necessary to perform and complete all audit procedures. The Third-Party Auditors shall execute Service Provider's "Confidentiality Agreement", substantially in the form attached hereto as Exhibit B, prior to the start of the audit. Client agrees that an audit conducted under this section will be conducted at such times and in a manner that avoids undue disruption of Service Provider's operations.

- 4.6.3. Books and Records. If required by Section 952 of the Omnibus Reconciliation Act of 1980, 42 U.S.C. Section 1395x(v)(1)(i) and (ii), for a period of four years after the Services are furnished, the parties agree to make available, upon the written request of the Secretary of Health and Human Services, the Comptroller General, or their representatives, this MA and such books, documents, and records as may be necessary to verify the nature and extent of the Services with a value or cost of \$10,000 or more over a twelve month period.

4.7. Warranties

4.7.1. Service Provider.

- (a) Prior to the Commencement Date. Unless Service Provider provided Services prior to the Commencement Date of any Service Schedule, Client will be responsible for all matters related to Client's practice prior to the Commencement Date, including, but not limited to, Client's billings, collections, third party reimbursements, accounts receivable and credit balances.
- (b) Disclaimer of Warranties. Service Provider disclaims any warranties or representations pertaining to the timing and amount of collections generated by the Services. Client acknowledges and agrees that Client is solely responsible for refunding any overpayments and processing any unclaimed property payments. Service Provider will provide Client with written notice of unresolved credit balances of which Service Provider becomes aware (such as overpayments or unclaimed property).
- (c) Other Warranties. Service Provider represents and warrants that:
  - (i) It will perform all of its obligations under the Agreement in a timely, professional and workmanlike manner, in accordance with all of the terms of the MA and the applicable Service Schedules;
  - (ii) The Services shall be provided using qualified personnel with suitable training, education, experience and skill to perform the Services in accordance with timing and other requirements of the Agreement; and
  - (iii) None of the Services or software provided to Client shall infringe any intellectual property rights of any third party or contain or involve any computer code, programs, procedures, mechanisms, or programming devices that are designed to, or would enable Service Provider or any third party to, disrupt, modify, delete, damage, deactivate, disable, harm, or otherwise impede in any manner the operation of the Client or any associated software, firmware, hardware, computer system, or network.



**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
Contract Number: RMS153968

**4.7.2. Client.****(a) Charges and Information.**

- (i) Client represents and warrants that it will forward to Service Provider (pursuant to the applicable Service Schedule[s]) only charges for which Client is entitled to bill. Client agrees to monitor and to refrain from knowingly submitting false or inaccurate information, charges, documentation or records to Service Provider and to ensure that the documentation provided by Client or an agent of Client to Service Provider supports the medical services provided by Client. Client acknowledges and agrees it has an obligation to report and correct any credible evidence of deficiencies on the part of Client. Client also acknowledges that Service Provider does not make a determination of medical necessity for any claims.
- (ii) Client acknowledges and agrees that Service Provider is not a collection agency. Client represents and warrants that any debt or account referred to Service Provider pursuant to this MA is not in default or delinquent or has not been written off as bad debt. If any accounts are found to be written off, in default or otherwise delinquent, Client agrees to immediately recall those accounts from Service Provider's responsibility under this MA.

- (b) Release of Information. Client represents and warrants that Client has obtained a release of information and insurance assignment of benefits from all individuals for whom Client is submitting charges to Service Provider for the provision of the Services and will immediately notify Service Provider if such release of information and insurance assignment of benefits is changed or revoked or if such individual refused/failed to execute such documents. Client further agrees to provide a copy of such signed documents upon Service Provider's request. The term "individuals" in this Section refers to the individual physicians/practitioners, or group members, on whose behalf the Client is directing Service Provider to submit claims.

- 4.8. Business Associate. The parties agree to the obligations set forth in Exhibit A.

- 4.9. Exclusion From Federal Healthcare Programs. Each party warrants that it is not currently listed by a Federal agency as excluded, debarred, or otherwise ineligible for participation in any Federal health care program. Each party agrees that it will not employ, contract with, or otherwise use the services of any individual whom it knows or should have known, after reasonable inquiry, (i) has been convicted of a criminal offense related to health care (unless the individual has been reinstated to participation in Medicare and all other Federal health care programs after being excluded because of the conviction), or (ii) is currently listed by a Federal agency as excluded, debarred, or otherwise ineligible for participation in any Federal health care program. Each party agrees that it will immediately notify the other in the event that it, or any person in its employ, has been excluded, debarred, or has otherwise become ineligible for participation in any Federal health care program. Each party agrees to continue to make reasonable inquiry regarding the status of its employees and independent contractors on a regular basis by reviewing the General Services Administration's List of Parties Excluded from Federal Programs and the HHS/OIG List of Excluded Individuals/Entities.

- 4.10. Governing Law. This MA is governed by and will be construed in accordance with the laws of the State of Michigan, exclusive of its rules governing choice of law and conflict of laws. Each party agrees that convenient venue for all actions, relating in any manner to this MA or any Service Schedule will be in a court of competent jurisdiction located in Oakland County, Michigan.

**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
Contract Number: RMS153968

- 4.11. Claims Period. Any action relating to this MA and any claim for damages, including, but not limited to, a claim for recurring damages arising out of the same cause or event, other than collection of outstanding payments, must be commenced within one year after the date upon which the cause of action occurred.
- 4.12. Assignment and Subcontracts. Neither party will assign this MA or its rights or obligations hereunder without the prior written consent of the other party, which will not be unreasonably withheld, delayed or conditioned. Service Provider may, upon notice to Client, assign this MA to any affiliate or to any entity resulting from the transfer of all or substantially all of Service Provider's assets or capital stock or from any other corporate reorganization. Service Provider may not subcontract its obligations under this MA to a subcontractor other than those listed in Exhibit F (each a "Permitted Off-Shore Subcontractor"). Service Provider agrees to hold its Permitted Off-Shore Subcontractors to the requirements in this MA as if Service Provider performed those Services itself, but Service Provider shall remain responsible for the performance of all of its obligations hereunder and shall be responsible for all acts, omissions, negligence and willful misconduct of its agents and subcontractors. Any change to the list of Permitted Off-Shore Subcontractors can be made only via written amendment to this MA which may include changes to services and pricing.
- 4.13. Severability. If any part of a provision of this MA is found illegal or unenforceable, it will be enforced to the maximum extent permissible, and the legality and enforceability of the remainder of that provision and all other provisions of this MA will not be affected.
- 4.14. Notices. All notices relating to the parties' legal rights and remedies under this MA will be provided in writing and will reference this MA. Such notices will be deemed given if sent by: (i) postage prepaid registered or certified U.S. Post mail, then five working days after sending; or (ii) commercial courier, then at the time of receipt confirmed by the recipient to the courier on delivery. All notices to a party will be sent to its address set forth on the cover page hereto, or to such other address as may be designated by that party by notice to the sending party.
- 4.15. Waiver. Failure to exercise or enforce any right under this MA will not act as a waiver of such right.
- 4.16. Force Majeure. Except for the obligation to pay money, a party will not be liable to the other party for any failure or delay caused in whole or in material part to any cause beyond its sole control, including but not limited to fire, accident, labor, dispute or unrest, flood, riot, war, rebellion, insurrection, sabotage, terrorism, transportation delays, shortage of raw materials, energy, or machinery, acts of God or of the civil or military authorities of a state or nation, or the inability, due to the aforementioned causes, to obtain necessary labor or facilities. In the event any of the foregoing events adversely affect Service Provider's ability to provide the Services required by this MA for more than 30 days, Client shall have the right to terminate this MA or any Service Schedule without any liability to Services Provider and/or use any third party to perform the Services for as long as an event of force majeure continues, and Client's obligations under this MA shall be reduced accordingly.
- 4.17. Amendment. This MA may be modified, or any rights under it waived, only by a written document executed by the authorized representatives of both parties. To avoid doubt, this MA may not be amended via electronic mail or other electronic messaging service.
- 4.18. No Third Party Beneficiaries. Except as specifically set forth in a Service Schedule, nothing in this MA will confer any right, remedy, or obligation upon anyone other than Client and Service Provider.
- 4.19. Relationship of Parties. Each party is an independent contractor of the other party. This MA will not be construed as constituting a relationship of employment, agency, partnership, joint venture or any other form of legal association. Neither party has any power to bind the other party or to assume or to create any obligation or responsibility on behalf of the other party or in the other party's name.

**CONFIDENTIAL AND PROPRIETARY**Client: Basha Diagnostics  
Contract Number: RMS153968

- 4.20. Non-solicitation of Employees. During the term of this MA and for a period of 12 months following the termination of this MA, each party agrees not to employ, contract with for services, solicit for employment on its own behalf or on behalf of any third party, or have ownership in any entity which employs or solicits for employment, any individual who (i) was an employee of the other or its parent, affiliates or subsidiaries at any time during the preceding 12 months and (ii) was materially involved in the provision or receipt of the Services hereunder without the prior written consent of the other party. Notwithstanding the foregoing, upon any termination of this MA, Client may rehire any individual who was employed by Client on the Effective Date, and who was hired by Service Provider on or after such date. Further, each party may place advertisements of general circulation (e.g., in newspapers, job search web sites, etc.) that are not specifically soliciting the individuals referenced above. Each party agrees that the other party may not have an adequate remedy at law to protect its rights under this Section and agrees that the non-defaulting party will have the right to seek injunctive relief from any violation or threatened violation of this Section.
- 4.21. Publicity. Neither party will make any other public announcement or press release regarding this MA or any activities performed hereunder without the prior written consent of the other party.
- 4.22. Construction of this MA. This MA will not be presumptively construed for or against either party. Section titles are for convenience only. As used in this MA, "will" means "shall," and "include" means "includes without limitation." The parties may execute this MA in one or more counterparts, each of which will be deemed an original and one and the same instrument.
- 4.23. Conflict Between MA and Schedules. In the event of any conflict or inconsistency in the interpretation of this MA (including its Service Schedules and all Amendments executed hereunder), such conflict or inconsistency will be resolved by giving precedence according to the following order: (a) the Amendment, (b) the Service Schedule, (c) the MA Terms and Conditions and Exhibits, (d) documents incorporated by reference.
- 4.24. Section Headings. The Section headings used herein are for convenience only and shall not be used in the interpretation of this MA.
- 4.25. Authority. Service Provider and Client represent and warrant that they have the full power and authority to enter into this MA, that there are no restrictions or limitations on their ability to perform this MA, and that the person executing this MA has the full power and authority to do so.
- 4.26. Entire Agreement. This MA, including Service Schedules, Exhibits, Amendments, and documents incorporated by reference, is the complete and exclusive agreement between the parties with respect to the subject matter hereof, superseding and replacing all prior agreements, communications, and understandings (written and oral) regarding its subject matter.

**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
Contract Number: RMS153968

**EXHIBIT A  
BUSINESS ASSOCIATE ADDENDUM**

This Business Associate Addendum ("Addendum") is entered into by and between PST Services, Inc. ("Business Associate") and Basha Diagnostics, P.C. ("Customer"). Business Associate and Customer may be individually referred to as a "Party" and, collectively, the "Parties" in this Addendum.

**SECTION 1: DEFINITIONS**

**"Breach"** will have the same meaning given to such term in 45 C.F.R. § 164.402.

**"Breach Notification Rule"** will mean the Notification in the Case of Breach of Unsecured Protected Health Information, 45 C.F.R. 164 subpart D.

**"Designated Record Set"** will have the same meaning as the term "designated record set" in 45 C.F.R. § 164.501.

**"Electronic Protected Health Information" or "Electronic PHI"** will have the meaning given to such term under the Privacy Rule and the Security Rule, including, but not limited to, 45 C.F.R. § 160.103, as applied to the information that Business Associate creates, receives, maintains or transmits from or on behalf of Customer.

**"Final Rule"** will mean a Final Omnibus Rule issued on January 25, 2013 by the Office of Civil Rights of the U.S. Department of Health and Human Services, implementing changes to, among other things, the Privacy Rule, Security Rule and Breach Notification Rule.

**"Individual"** will have the same meaning as the term "individual" in 45 C.F.R. § 160.103 and will include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

**"Privacy Rule"** will mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and E.

**"Protected Health Information" or "PHI"** will have the same meaning as the term "protected health information" in 45 C.F.R. § 160.103, as applied to the information created, received, maintained or transmitted by Business Associate from or on behalf of Customer.

**"Required by Law"** will have the same meaning as the term "required by law" in 45 C.F.R. § 164.103.

**"Secretary"** will mean the Secretary of the Department of Health and Human Services or his or her designee.

**"Security Incident"** will have the meaning given to such term in 45 C.F.R. § 164.304.

**"Security Rule"** will mean the Security Standards at 45 C.F.R. Part 160 and Part 164, Subparts A and C.

**"Underlying Agreement"** will mean the service agreement to which this Addendum is attached including all contract supplements and sales orders entered into as a part of or pursuant to such agreement, all as amended.

**"Unsecured PHI"** will have the same meaning given to such term under 45 C.F.R. § 164.402, and guidance promulgated thereunder.

**Capitalized Terms.** Capitalized terms used in this Addendum and not otherwise defined herein will have the meanings set forth in the Privacy Rule, the Security Rule, and the Final Rule, which definitions are incorporated in this Addendum by reference.



**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
Contract Number: RMS153968

**SECTION 2: PERMITTED USES AND DISCLOSURES OF PHI**

2.1 Uses and Disclosures of PHI Pursuant to the Underlying Agreement. Except as otherwise limited in this Addendum, Business Associate may use or disclose PHI only to perform functions, activities or services for, or on behalf of, Customer as specified in the Underlying Agreement or as Required by Law, provided that such use or disclosure would not violate the Privacy Rule if done by Customer.

2.2 Permitted Uses of PHI by Business Associate. Except as otherwise limited in this Addendum, Business Associate may use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.

2.3 Permitted Disclosures of PHI by Business Associate. Except as otherwise limited in this Addendum, Business Associate may disclose PHI for the proper management and administration of Business Associate, provided that the disclosures are Required by Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person (which purpose must be consistent with the limitations imposed upon Business Associate pursuant to this Addendum), and that the person agrees to notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached. Business Associate may disclose PHI to report violations of law to appropriate federal and state authorities, consistent with 45 C.F.R. § 164.502(j)(1).

2.4 Data Aggregation. Except as otherwise limited in this Addendum, Business Associate may use PHI to provide Data Aggregation services for the Health Care Operations of the Customer as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).

2.5 De-identified Data. Business Associate may de-identify PHI in accordance with the standards set forth in 45 C.F.R. § 164.514(b) and may use or disclose such de-identified data unless prohibited by applicable law.

**SECTION 3: OBLIGATIONS OF BUSINESS ASSOCIATE**

3.1 Appropriate Safeguards. Business Associate will use appropriate safeguards and will, after the compliance date of the HIPAA Final Rule, comply with the Security Rule with respect to Electronic PHI, to prevent use or disclosure of such information other than as provided for by the Underlying Agreement and this Addendum. Except as expressly provided in the Underlying Agreement or this Addendum, Business Associate will not assume any obligations of Customer under the Privacy Rule. To the extent that Business Associate is to carry out any of Customer's obligations under the Privacy Rule as expressly provided in the Underlying Agreement or this Addendum, Business Associate will comply with the requirements of the Privacy Rule that apply to Customer in the performance of such obligations.

3.2 Reporting of Improper Use or Disclosure, Security Incident or Breach. Business Associate will report to Customer any use or disclosure of PHI not permitted under this Addendum, Breach of Unsecured PHI or any Security Incident, without unreasonable delay, and in any event no more than ten (10) business days following discovery; provided, however, that the Parties acknowledge and agree that this Section constitutes notice by Business Associate to Customer of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below). "Unsuccessful Security Incidents" will include, but not be limited to, pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of PHI. Business Associate's notification to Customer of a Breach will include: (i) the identification of each individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired or disclosed during the Breach; and (ii) any particulars regarding the Breach that Customer would need to include in its notification, as such particulars are identified in 45 C.F.R. § 164.404. Further, to the extent Required by Law, Business Associate shall provide Customer with any other available information that Customer is required to include in notification to Individual as information becomes available, even if it becomes available after the required notifications have been sent to the affected individuals or after the 10-day period specified above has elapsed. Business Associate shall take prompt corrective action to cure any such Breach.

**CONFIDENTIAL AND PROPRIETARY**Client: Basha Diagnostics  
Contract Number: RMS153968

**3.3 Cost Reimbursement.** To the extent (i) any Breach is caused by Business Associate or any of its employees, agents, or subcontractors, and the Breach Notification Rule requires notice to Individuals and/or media pursuant to 45 C.F.R. §§ 164.404 and/or 164.406, or (ii) Business Associate or any of its employees, agents, or subcontractors fail to comply with any provisions of this Addendum, the Privacy Rule or the Security Rule, then Business Associate agrees to reimburse Customer for the reasonable and substantiated costs related to the following: providing notifications to the media, the Secretary and the affected Individuals, providing credit monitoring services to the affected individuals, if appropriate, for up to one year, any fines and penalties assessed against Customer directly attributable to a Breach or other violation of this Addendum, the Privacy Rule and/or Security Rule by Business Associate or any of its employees, agents or subcontractors, investigation costs, attorneys' fees, and mitigation efforts required under the Privacy Rule or Security Rule. If the parties agree that Business Associate will send or cause to be sent notifications to affected Individuals, Business Associate will comply with the requirements pursuant to 45 C.F.R. § 164.404 and will provide Covered Entity with an advance copy of the proposed letter for review and approval prior to sending to the affected Individuals.

**3.4 BUSINESS ASSOCIATE'S TOTAL CUMULATIVE LIABILITY IN CONNECTION WITH THIS ADDENDUM IS EXPRESSLY SUBJECT TO THE LIMITATION OF LIABILITY SET FORTH IN THE UNDERLYING AGREEMENT GOVERNING THE APPLICABLE SERVICE OR PRODUCT.**

**3.5 Business Associate's Agents.** In accordance with 45 C.F.R. § 164.502(e)(1)(ii) and 45 C.F.R. § 164.308(b)(2), as applicable, Business Associate will enter into a written agreement with any agent or subcontractor that creates, receives, maintains or transmits PHI on behalf of Business Associate for services provided to Customer, providing that the agent or subcontractor agrees to restrictions and conditions that are substantially the same as those that apply through this Addendum to Business Associate with respect to such PHI and agrees to comply with the applicable requirements of the Security Rule. If Business Associate knows of a pattern of activity or practice of an agent or subcontractor that constitutes a material breach or violation of the agent or subcontractor's obligation under the contract or other arrangement, Business Associate shall take reasonable steps to cure the breach or end the violation, as applicable, and if such steps are unsuccessful, terminate the contract or agreement, if feasible.

**3.6 Access to PHI.** The Parties do not intend for Business Associate to maintain any PHI in a Designated Record Set for Customer. To the extent Business Associate possesses PHI in a Designated Record Set, Business Associate agrees to make such information available to Customer pursuant to 45 C.F.R. § 164.524, within ten (10) business days of Business Associate's receipt of a written request from Customer; provided, however, that Business Associate is not required to provide such access where the PHI contained in a Designated Record Set is duplicative of the PHI contained in a Designated Record Set possessed by Customer. If an Individual makes a request for access pursuant to 45 C.F.R. § 164.524 directly to Business Associate, or inquires about his or her right to access, Business Associate will either timely forward such request to Customer or direct the Individual to Customer.

**3.7 Amendment of PHI.** The Parties do not intend for Business Associate to maintain any PHI in a Designated Record Set for Customer. To the extent Business Associate possesses PHI in a Designated Record Set, Business Associate agrees to make such information available to Customer for amendment pursuant to 45 C.F.R. § 164.526 within ten (10) business days of Business Associate's receipt of a written request from Customer. If an Individual submits a written request for amendment pursuant to 45 C.F.R. § 164.526 directly to Business Associate, or inquires about his or her right to amendment, Business Associate will either forward such request to Customer or direct the Individual to Customer.

**3.8 Documentation of Disclosures.** Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Customer to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. Business Associate will document, at a minimum, the following information ("Disclosure Information"): (a) the date of the disclosure; (b) the name and, if known, the address of the recipient of the PHI; (c) a brief description of the PHI disclosed; (d) the purpose of the disclosure that includes an explanation of the basis for such disclosure; and (e) any additional information required under the HITECH Act and any implementing regulations.

**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
Contract Number: RMS153968

**3.9 Accounting of Disclosures.** Business Associate agrees to provide to Customer, within ten (10) business days of Business Associate's receipt of a written request from Customer, information collected in accordance with Section 3.6 of this Addendum, to permit Customer to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. If an Individual submits a written request for an accounting of disclosures of PHI pursuant to 45 C.F.R. § 164.528 directly to Business Associate, or inquires about his or her right to an accounting, Business Associate will direct the Individual to Customer.

**3.10 Governmental Access to Records.** Business Associate will make its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Customer available to the Secretary in the time and manner requested by the Secretary, for purposes of the Secretary determining Business Associate's or Customer's compliance with the Privacy Rule and the Security Rule, and shall notify Customer within ten (10) business days of any request it receives from the Secretary that in any way relates to the Underlying Agreement.

**3.11 Mitigation.** To the extent practicable, Business Associate will cooperate with Customer's efforts to, and where Required by Law shall also, mitigate a harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate or any of its agents or subcontractors that is not permitted by this Addendum.

**3.12 Minimum Necessary.** Business Associate will request, use and disclose the minimum amount of PHI necessary to accomplish the purpose of the request, use or disclosure, in accordance with 45 C.F.R. § 164.514(d), and any amendments thereto, and any such use, disclosure or request shall comply with the Secretary's guidance on the minimum necessary standard in accordance with section 13405(b) of the HITECH Act as of its effective date.

**3.13 HIPAA Final Rule Applicability.** Business Associate acknowledges that enactment of the HITECH Act, as implemented by the HIPAA Final Rule, amended certain provisions of HIPAA in ways that now directly regulate, or will on future dates directly regulate, Business Associate under the Privacy Rule and Security Rule. Business Associate agrees, as of the compliance date of the HIPAA Final Rule, to comply with applicable requirements imposed under the HIPAA Final Rule, including any amendments thereto.

**3.14 Prohibited Uses and Disclosures.** Business Associate shall not:

3.14.1 Make or cause to be made any Marketing or Fundraising communication that involves or is based on, in whole or in part, any PHI, without a prior written consent of Customer; or

3.14.2 Disclose PHI to a health plan for Payment or Health Care Operations purposes which is not otherwise Required by Law, if (i) Customer has advised Business Associate no later than ten (10) business days from the request that the Individual has requested of Customer this special restriction or the Individual has directly notified Business Associate of this restriction, and (ii) Business Associate has knowledge that the PHI pertains solely to a health care item or service for which the Individual, or another person on behalf of the Individual other than the health plan, has paid Customer out of pocket in full; or

3.14.3 Directly or indirectly receive remuneration in exchange for PHI created, received, maintained or transmitted as prohibited by 45 CFR 164.502(a)(5)(ii); provided, however, that this shall not affect payment by Customer to Business Associate for Services under the Underlying Agreement or other disclosures that do not constitute a Sale of PHI under the HIPAA Privacy Rule.

**3.15 Transactions.** If Business Associate conducts electronic Transactions on behalf of Customer for which the U.S. Department of Health and Human Services has established standards, Business Associate, to the extent Required by Law, shall comply, and shall require its agents and subcontractors involved with the conduct of such Transactions to comply, with the applicable requirements of the Electronic Transactions Rule. Business Associate will also, to the extent Required by Law, comply with the other requirements of 45 CFR Part 162.

**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
Contract Number: RMS153968

**SECTION 4: OBLIGATIONS OF CUSTOMER**

**4.1 Notice of Privacy Practices.** Customer will notify Business Associate of any limitation(s) in its notice of privacy practices in accordance with 45 C.F.R. § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI. Customer will provide such notice no later than fifteen (15) days prior to the effective date of the limitation.

**4.2 Notification of Changes Regarding Individual Permission.** Customer will obtain any consent or authorization that may be required by the Privacy Rule, or applicable state law, prior to furnishing Business Associate with PHI. Customer will notify Business Associate no later than five (5) days prior to the effective date of the limitation of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI. To the extent that notification by an Individual under this section does not allow Customer to provide at least five (5) days prior notice to Business Associate, Customer shall notify Business Associate as soon as practicable after receiving notice from the Individual and Business Associate will take the necessary steps to comply with the Individual's request as soon as reasonably possible.

**4.3 Notification of Restrictions to Use or Disclosure of PHI.** Customer will notify Business Associate no later than five (5) days prior to the effective date of the limitation of any restriction to the use or disclosure of PHI that Customer has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI. To the extent that notification by an Individual under this section does not allow Customer to provide at least five (5) days prior notice to Business Associate, Customer shall notify Business Associate as soon as practicable after receiving notice from the Individual and Business Associate will take the necessary steps to comply with the Individual's request as soon as reasonably possible. If Business Associate reasonably believes that any restriction agreed to by Customer pursuant to this Section may materially impair Business Associate's ability to perform its obligations under the Underlying Agreement or this Addendum, the Parties will mutually agree upon any necessary modification of Business Associate's obligations under such agreements.

**4.4 Permissible Requests by Customer.** Customer will not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule, the Security Rule or the HITECH Act if done by Customer, except as permitted pursuant to the provisions of Sections 2.2, 2.3, 2.4 and 2.5 of this Addendum.

**SECTION 5: TERM AND TERMINATION**

**5.1 Term.** The term of this Addendum will commence as of the Effective Date of the Underlying Agreement, and will terminate when all of the PHI provided by Customer to Business Associate, or created or received by Business Associate on behalf of Customer, is destroyed or returned to Customer. If it is infeasible to return or destroy PHI, Business Associate will extend the protections to such information, in accordance with Section 5.3.

**5.2 Termination for Cause.** Upon either Party's knowledge of a material breach by the other Party of this Addendum, such Party may terminate this Addendum immediately if cure is not possible. Further, Customer may terminate this Addendum and the Underlying Agreement immediately in the event of a Breach involving 500 or more patients of the Customer caused by the Service Provider or any of its employees, agents, or subcontractors. Otherwise, the non-breaching party will provide written notice to the breaching Party detailing the nature of the breach and providing an opportunity to cure the breach within thirty (30) business days. Upon the expiration of such thirty (30) day cure period, the non-breaching Party may terminate this Addendum and the Underlying Agreement if the breaching party does not cure the breach or if cure is not possible.

**5.3 Effect of Termination.**

**5.3.1** Except as provided in Section 5.3.2, upon termination of the Underlying Agreement or this Addendum for any reason, Business Associate will return or, at Customer's request, destroy all PHI received from Customer, or created or received by Business Associate on behalf of Customer, and will retain no copies of the PHI, provided further that (i) if Customer elects destruction of the PHI, Business



**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
Contract Number: RMS153968

Associate shall destroy such PHI at no cost to the Customer and certify same in writing, and (ii) if Customer requires Business Associate to return any of the PHI then Customer shall reimburse Business Associate for the reasonable costs incurred by Business Associate attributable directly to returning the PHI, provided that Customer is notified of and approves such costs before Business Associate incurs them. This provision will apply to PHI that is in the possession of subcontractors or agents of Business Associate.

5.3.2 If it is infeasible for Business Associate to return or destroy the PHI upon termination of the Underlying Agreement or this Addendum, Business Associate will: (a) extend the protections of this Addendum to such PHI and (b) limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI. This provision will apply to PHI that is in the possession of subcontractors or agents of Business Associate.

**SECTION 6: COOPERATION IN INVESTIGATIONS**

The Parties acknowledge that certain breaches or violations of this Addendum may result in litigation or investigations pursued by federal or state governmental authorities of the United States resulting in civil liability or criminal penalties. Each Party will cooperate in good faith in all respects with the other Party in connection with any request by a federal or state governmental authority for additional information and documents or any governmental investigation, complaint, action or other inquiry.

**SECTION 7: SURVIVAL**

The respective rights and obligations of Business Associate under Sections 3.3 and 5.3 of this Addendum will survive the expiration or termination of this Addendum and/or the Underlying Agreement for any reason.

**SECTION 8: AMENDMENT**

This Addendum may be modified, or any rights under it waived, only by a written document executed by the authorized representatives of both Parties. In addition, if any relevant provision of the Privacy Rule, the Security Rule or the HIPAA Final Rule is amended in a manner that changes the obligations of Business Associate or Customer that are embodied in terms of this Addendum, then the Parties agree to negotiate in good faith appropriate non-financial terms or amendments to this Addendum to give effect to such revised obligations.

**SECTION 9: EFFECT OF ADDENDUM**

In the event of any inconsistency between the provisions of this Addendum and the Underlying Agreement, the provisions of this Addendum will control. In the event that a court or regulatory agency with authority over Business Associate or Customer interprets the mandatory provisions of the Privacy Rule, the Security Rule or the HIPAA Final Rule, in a way that is inconsistent with the provisions of this Addendum, such interpretation will control. Where provisions of this Addendum are different from those mandated in the Privacy Rule, the Security Rule, or the HIPAA Final Rule, but are nonetheless permitted by such rules as interpreted by courts or agencies, the provisions of this Addendum will control.

**SECTION 10: GENERAL**

This Addendum is governed by, and will be construed in accordance with, the laws of the State that govern the Underlying Agreement. Any action relating to this Addendum must be commenced within one year after the date upon which the cause of action accrued. Neither party may assign this Addendum or its rights or obligations hereunder without the prior written consent of the other party, which will not be unreasonably withheld. If any part of a provision of this Addendum is found illegal or unenforceable, it will be enforced to the maximum extent permissible, and the legality and enforceability of the remainder of that provision and all other provisions of this Addendum will not be affected. All notices relating to the Parties' legal rights and remedies under this Addendum will be provided in writing to a Party, will be sent to its address set forth in the Underlying Agreement, or to such other address as may be designated by that Party by notice to the sending Party, and will reference this Addendum. Nothing in this Addendum will confer any right, remedy, or obligation upon anyone other than Customer and Business Associate. This

**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
Contract Number: RMS153968

Addendum is the complete and exclusive agreement between the Parties with respect to the subject matter hereof, superseding and replacing all prior agreements, communications, and understandings (written and oral) regarding its subject matter

**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
 Contract Number: RMS153968  
 SAP Customer Number:

**EXHIBIT B  
 CONFIDENTIALITY AGREEMENT**

Service Provider and Basha Diagnostics ("Client") have entered into an agreement whereby Service Provider provides certain services (the "Services") to Client (the "Master Services Agreement"). Client has entered into a contractual relationship with           [insert name of person/entity performing the audit]           ("Recipient") and instructs Service Provider to allow Recipient to review certain information in Service Provider's possession regarding Client's business and accounts receivable billing and collections performed by Service Provider ("Client Proprietary Information"). Therefore, in consideration of the mutual covenants and conditions contained in this Confidentiality Agreement (the "Confidentiality Agreement"), Recipient and Client agree as follows:

A. During the course of Recipient's examination and review of Client Proprietary Information, Recipient may be exposed to or review certain proprietary information regarding Service Provider ("Service Provider Proprietary Information"). Service Provider Proprietary Information refers to any and all data and information relating to the business of Service Provider which has value to Service Provider and is not generally known by its competitors or the public, including, without limitation, financial information, inventions, methods, techniques, actual or potential customers and suppliers, the Master Services Agreement, Service Provider's business practices or other trade secrets or confidential information of Service Provider, all report formats, and existing and future products and computer systems and software. Recipient acknowledges and agrees that all Service Provider Proprietary Information and all physical embodiments thereof are confidential to Service Provider and are and will remain the sole and exclusive property of Service Provider. All Service Provider Proprietary Information acquired by Recipient will be kept strictly confidential and will not be disclosed to any other person or entity (including any entity affiliated with or any division of Recipient).

B. Service Provider Proprietary Information does not include information which (i) is publicly known or which becomes publicly known through no act or failure to act on the part of Recipient; (ii) is lawfully obtained by Recipient from any third party entitled to disclose such information; (iii) is in the lawful possession of Recipient prior to such information having been disclosed to Recipient by Service Provider; or (iv) is independently developed by Recipient.

C. Recipient further agrees that during Recipient's engagement by Client and for a period of one (1) year following any termination of Recipient's engagement for whatever reason, Recipient will not, directly or indirectly, on Recipient's own behalf or in the service of, or on behalf of any other individual or entity, divert, solicit or hire away, or attempt to divert, solicit or hire away, to or for any individual or entity, any person employed by Service Provider, whether or not such employee is a full-time employee, temporary employee, leased employee or independent contractor of Service Provider, whether or not such employee is employed pursuant to written agreement and whether or not such employee is employed for a determined period or at-will.

D. Recipient acknowledges that great loss and irreparable damage would be suffered by Service Provider if Recipient should breach or violate the terms of this Confidentiality Agreement. In the event Recipient breaches or violates this Confidentiality Agreement, Recipient agrees that Service Provider may not have an adequate remedy at law and, therefore, that Service Provider would be entitled to seek a temporary restraining order and permanent injunction to prevent a breach of any of the terms or provisions contained in this Confidentiality Agreement, in addition to any monetary damages that may be available at law or equity. Recipient's obligations under this Confidentiality Agreement will survive indefinitely.

E. Recipient represents and warrants that (i) it has the full power and authority to enter into this Confidentiality Agreement, and (ii) the person executing this Confidentiality Agreement has the full power and authority to do so.

IN WITNESS WHEREOF, Recipient has signed this Confidentiality Agreement as of the date below written.

**RECIPIENT:**

By:

Printed Name:

Title:

Date:

**SAMPLE**  
 (No Signature Required)

**CLIENT:**

By:

Printed Name:

Title:

Date:

**Basha Diagnostics**

**SAMPLE**  
 (No Signature Required)

**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
Contract Number: RMS153968  
SAP Customer Number:

**EXHIBIT C  
TRANSITION SPECIFICS**

Upon termination or expiration of this MA or any Service Schedule referenced in the MA, for any reason, Service Provider agrees to provide at no charge to the Client the following assistance to Client or Client's designated agent to transfer Service Provider's responsibilities under this MA and Service Schedule to Client or Client's designated agent "Transitional Services"):

**Data Specifications** Patient information will be provided via a write-protected CD.  
Detailed specifications will be provided to Client or Client's designated agent:

**Technical and Operational contacts** Service Provider Support contacts will be provided to answer questions regarding the specifications document and operational requirements. Questions may be presented by Client or its designee.

**Test CD** A test CD will be provided containing 100 patient accounts and their associated transaction activity.

**Final CD** A final CD will include all debit and credit balance accounts residing in the active AR. Zero balance accounts will be provided up to the age of two years (based on the date the account was placed on the system). Patient demographic and transaction information is included.

**Utility File Codes** Listings will be provided to Client or its designee for the following files:  
Change codes, description and CPT  
Referring physician code, name and NPI (if available)  
Performing physician, code and name  
Location of service, code and description  
Transaction codes and description

and such other transition support services as may be reasonably requested by the Client.



**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
 Contract Number: RMS153968  
 SAP Customer Number:

**EXHIBIT D**  
**END USER TERMS AND CONDITIONS**

I. Client acknowledges and agrees that all Services, computer software, programs, specifications and designs, documentation, manuals, methodologies, processes, and other materials, information, and the content of the foregoing accessed by Client that is provided by or on behalf of Service Provider or its licensors, and any copies thereof, (the "PST Proprietary and Confidential Information") are the proprietary, confidential and trade secret information of Service Provider, or its licensors, and shall remain so; and that such PST Proprietary and Confidential Information may be utilized by Client only to facilitate its use of the Services in accordance with the terms of this Exhibit and the MA. Client agrees, and will cause its employees, agents and representatives to agree, that it/they (i) shall not copy, modify, change, disassemble, or reverse engineer any PST Proprietary and Confidential Information, and (ii) shall not disclose PST Proprietary and Confidential Information, except as legally required. Data from transactions received or created by Service Provider may be utilized by Service Provider for data aggregation and/or statistical compilations or reports, research, and for other purposes (the "Uses") so long as such Uses are in compliance with all applicable laws and patient identifying information is de-identified consistent with the HIPAA Privacy Rule, and such Uses shall be the sole and exclusive property of Service Provider. The parties agree not to disclose the terms of this Exhibit, either party's business practices or other trade secrets or confidential and trade secret information of the other party or its licensors, except as legally required.

II. Client agrees, and shall cause its employees, agents and representatives to agree, that it/they shall not intentionally: (a) transmit or share identification and/or password codes to persons other than the Authorized Users for whom such codes were generated; (b) permit Authorized Users to share identification and/or password codes with others; (c) permit the identification and/or password codes from being cached in proxy servers and accessed by individuals who are not Authorized Users; (d) permit access to the Software through a single identification and/or password code being made available to multiple users on a network; or (e) attempt or permit any person without valid identification and/or password codes to attempt to access the Software. Client agrees that (w) the Software embodies valuable and proprietary trade secrets of Service Provider and/or its licensors, (x) the identification and password codes issued by Service Provider hereunder constitute valuable confidential information, which is proprietary to Service Provider, (y) any reports, report formats, documents, ideas or other discoveries made or developed by Client during its use of the Software may be utilized by Client only at the Client facility where it is installed, only to facilitate its use of the Services hereunder in accordance with the terms of this Exhibit and the MA, only in accordance with user instructions and specifications provided by Service Provider and shall not be given or sold to or used on behalf of any third-party, and any reports, report formats, documents, ideas or other discoveries shall remain the sole and exclusive property of Service Provider, and (z) Client agrees, and will cause its employees, agents, subcontractors and representatives to agree, that it/they shall not copy, modify, change, disassemble, or reverse engineer any part or aspect of the Software.

III. The Software shall be in machine-readable object code and may only be utilized at the Client facility where it is installed, solely for Client transactions for which Service Provider is to perform the Services, and only in accordance with user instructions and specifications provided by Service Provider. Client shall obtain and maintain, at no cost or expense to Service Provider, the software/hardware required by Client to access the Software and acknowledges that Service Provider recommends no specific manufacturer and/or software that complies with its specifications. As between Service Provider and Client, all such Software is acknowledged to be subject to Section V of this Exhibit and the MA. EXCEPT AS OTHERWISE PROVIDED IN THE MA, SERVICE PROVIDER MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESSED OR IMPLIED, WITH RESPECT TO THE SOFTWARE AND DISCLAIMS ALL OTHER WARRANTIES, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE.

IV. Client users shall access the Software through a combination of user names and passwords as necessary to provide appropriate security. Client shall be solely responsible for assigning user names and passwords to its users and for strictly maintaining the confidentiality of such user names and passwords. Client shall ensure that all of its users comply with all of the terms and conditions of this Exhibit and the MA. Client shall not permit any person or entity, other than its designated users, to use or gain access to the Services and shall provide reasonable safeguards to protect against unauthorized usage of or access to the Services.

**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
Contract Number: RMS153968  
SAP Customer Number:

V. Client shall not use the Software in any manner, or in connection with any Client specific materials that (i) infringes upon or violates any intellectual property right of any third-party, (ii) constitutes a defamation, libel, invasion of privacy, or violation of any right of publicity or other third-party right or is threatening, harassing or malicious, or (iii) violates any applicable international, federal, state or local law, rule, legislation, regulation or ordinance, including without limitation, the Communications Decency Act of 1996, as amended, and will not initiate or otherwise pursue development efforts that attempt to duplicate or re-create any functionality, processes or business model concepts included in the Software.

VI. Service Provider reserves the right to substitute alternative products providing equivalent core functionality to the Software.

VII. Upon Client's ceasing use of the Software, the termination of this Exhibit and the MA, or Service Provider's written request, Client shall cease using all Service Provider provided Software and related materials and promptly return same to Service Provider at Service Provider's expense. Client shall certify to Service Provider in writing that all copies (in any form or media) of the materials received, whether or not modified or incorporated into other materials, have been destroyed or returned to Service Provider. Termination of this Exhibit and the MA or any license shall not relieve Client's obligation to pay all fees incurred prior to such termination and shall not limit either party from pursuing any other remedies available to it.

VIII. Each party agrees that the other party and/or its licensors may not have an adequate remedy at law to protect their respective rights under this Exhibit and will have the right to seek injunctive relief from any violation or threatened violation of this Exhibit with respect to their respective rights.

**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
 Contract Number: RMS153968  
 SAP Customer Number:

- 3.1.2. Fee for Physician Enrollment. Service Provider will provide enrollment Services for (a) 20 physicians, and (b) five additional physicians per year of the MA, at no cost to Client. Any enrollment over the amount specified previously, Client agrees to pay Service Provider an amount equal to \$500.00 per physician per payer for Service Provider's provision of enrollment and/or re-enrollment Services for Client.
- 3.1.3. Fee for Postage. Client agrees to pay Service Provider an amount equal to the postage charges related to the Services provided during the previous month, including any increase in the cost of postage paid by Service Provider arising out of any increase in the U.S. Postal Service rates after the Commencement Date.
- 3.2. Net Collections. Net Collections means the total sum of all monies collected by Client directly as a result of Service Provider's performance of the Services on Client's behalf, less amounts refunded or credited to a patient or third party payer as a result of overpayments, erroneous payments or bad checks. Further, Net Collections do not include, and the calculation of Service Provider's compensation hereunder shall not be based on, any amounts collected by Client or Service Provider on Client's accounts receivable that existed prior to the Effective Date of the MA or any amounts collected with an involvement of a collection agency or legal counsel engaged for purposes of pursuing the collection.
- 3.3. Global/Technical/Purchased Service/Place of Service. Client represents that it is entitled to bill, and directs Service Provider to bill on its behalf, (a) globally, (b) for the technical component, including supplies, or (c) for purchased services. In furtherance of this request, Client will complete the Application For Global/Technical/Purchased Services Billing during the implementation process.
- Client will complete the Place of Service Form during the implementation process instructing Service Provider to bill its accounts as a facility and/or non-facility place of service.
- 3.4. Practice Assumptions. The following assumptions are based on information Client has provided to Service Provider. Based on these assumptions, Service Provider has derived the schedule of fees set forth above.

- |    |   |           |
|----|---|-----------|
| 1. | Average Net Collections per month:      | \$783,333 |
| 2. | Average number of procedures per month: | 4,925.    |

Notwithstanding the foregoing, the above amounts are estimates only, and Client makes no representation or warranty with respect to the average or actual Net Collections per month, the average or actual number of procedures per month, or with respect to any other matter related to any type or volume of procedures, collections or any other matter that may exist following the execution of the MA, including the volume of the Services that Service Provider will provide under the MA or any Service Schedule.

**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
 Contract Number: RMS153968  
 SAP Customer Number:

**SERVICE SCHEDULE 2****Scope of Services - MCKESSON PRACTICE FOCUS WEB BASED REPORTING SERVICES**

The MA Terms and Conditions and this Service Schedule apply to the McKesson Practice Focus Web Based Reporting Services rendered by Service Provider under this Service Schedule.

**1. TERM**

- 1.1. Initial Term of Schedule. The initial term of this Service Schedule is two years (the "Schedule Term") beginning September 1, 2016 (the "Commencement Date").
- 1.2. Termination. Either party may terminate this Service Schedule at any time following the expiration of the initial Schedule Term upon sixty (60) days prior written notice to the other party.
- 1.3. Automatic Renewal. This Service Schedule will automatically renew for one year terms unless (i) either party delivers to the other written notice of termination at least 90 days prior to the expiration of the then-current term, or (ii) as otherwise set forth in the MA.

**2. SCOPE OF SERVICES**

- 2.1. Responsibilities. Each party agrees to perform its respective responsibilities identified below in a timely and diligent manner. Client acknowledges and agrees that Service Provider's performance of the McKesson Practice Focus Web Based Reporting Services is dependent upon Client's performance of its responsibilities as set forth in this Service Schedule.

**2.1.1. Service Provider Responsibilities.**

- (a) Basic User Access.
  - (i) Provide 24 hour access, less scheduled or unscheduled downtime for maintenance or repair, from any Internet access point to the Client reporting portal at Customer Login at McKesson.com.
  - (ii) Provide access to all current and future standard level reports generated by Service Provider.
  - (iii) Provide ability to review reports as HTML and PDF documents.
  - (iv) Provide the ability to save report documents as PDF, Excel or CSV file formatted documents.
  - (v) Provide access to the Dashboard folder and associated current and future Dashboard based deliverables.
- (b) Intermediate User Access.
  - (i) Includes all activities defined in the Basic User Access.
  - (ii) Provide access to all current and future public reports generated by Service Provider.
  - (iii) Provide online analysis functionality which allows Client the ability to drill down, filter and group data as well as apply simple updates such as adding/removing fields, re-sorting, calculations, etc.
  - (iv) Provide a personal reporting mail box which enables Client to send/receive reports to/from other users within Client group.
  - (v) Provide ability to save in a personal folder a copy of an altered report for future data refresh or editing.
  - (vi) Provide the ability to schedule saved reports as needed.
- (c) Advanced User Access.
  - (i) Includes all activities as defined in the Basic and Intermediate User Access.
  - (ii) Provide ability to create, edit and save document structures and formats.

**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
 Contract Number: RMS153968  
 SAP Customer Number:

- (iii) Provide ability to manipulate report query, prompts, filters and scope of analysis.
  - (iv) Provide ability to modify/create formulas and report variables.
  - (v) Provide access to Service Provider's complete ad-hoc reporting development framework.
  - (vi) Provide the ability to customize reporting queries.
  - (vii) Provide the ability to set personal user reporting preferences.
  - (viii) Upon Client request, provide a Client named folder to be utilized by Client appointed Advanced User(s) to store reports for Client use.
- (d) Support Services. Service Provider will provide telephone and e-mail support to answer questions and address issues related to the Practice Focus Web Based Reporting product at no cost to Client. Normal support hours and response time are as follow:
- Monday through Friday: 8:00 a.m. until 8:00 p.m. eastern time
- (e) Training Services. Service Provider will provide Client with one 1-hour webinar for Basic Users on the Practice Focus Web Based Reporting Product at no cost to Client. Recommended training for Intermediate Users is either a 2-day on-site Intermediate training session or attendance at a public Intermediate training session. Recommended training for Advanced Users is attendance at an Intermediate training session and additional attendance at either a 2-day on-site Advanced training session or attendance of a public Advanced training session. Service Provider can provide Client training classes for a specific Client environment or as specifically requested by Client. All Training Services provided at Client's site(s) shall be performed by Service Provider's or its affiliate's employees or representatives who are based in the Metro Detroit area. Further, all Training Services that will be provided at the Service Provider's facility shall be provided in the Service Provider's or its affiliate's facility located in Metro Detroit area.
- (f) eLearning Training For Intermediate User Access. If requested by Client's "Manager," Service Provider will provide a one year subscription for Intermediate User(s) at the fees set forth in this Service Schedule.
- (g) Mobile Electronic Authorized User Access. If requested by Client's "Manager," Service Provider will provide Client an Authorized User and allow such Authorized User to access McKesson Practice Focus by means of an I-Pad or other mobile electronic device authorized by Service Provider at the fees set forth in this Service Schedule.
- (h) Consulting Services. If requested by Client's "Manager," Service Provider's staff of resources can design, build and generate customized Client specific Practice Focus deliverables, including but not limited to customized reports, graphs and dashboards at the fees set forth in this Service Schedule.
- 2.1.2. Client Responsibilities. Client will:
- (a) Establish Client's broadband access to the Internet for use of the Practice Focus Web Based Reporting product.
  - (b) Allow access to such Practice Focus Web Based Reporting Product only to user(s) authorized by Service Provider to access and use such Practice Focus Web Based Reporting Product ("Authorized User").



**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
 Contract Number: RMS153968  
 SAP Customer Number:

- (c) Provide a competent member of Client's staff ("Manager") to be trained by Service Provider on use of the Practice Focus Web Based Reporting product to serve as a liaison to Service Provider on Practice Focus Web Based Reporting matters.
- (d) After Service Provider has provided training to the Client's Manager, Client agrees to train only other Authorized Users on use of the Practice Focus Web Based Reporting product.
- (e) Client's Manager may change Authorized Users level of use or add or subtract Authorized Users on no less than 15 days' prior written notice to Service Provider (e-mail requests are acceptable). Client will pay Service Provider the applicable pro-rated Authorized User fee for any Authorized User added or subtracted during any month.
- (f) Client acknowledges and agrees that it shall not intentionally: (i) transmit or share identification and/or password codes to persons other than the Authorized Users for whom such codes were generated; (ii) permit Authorized Users to share identification and/or password codes with others; (iii) permit the identification and/or password codes from being cached in proxy servers and accessed by individuals who are not Authorized Users; (iv) permit access to the McKesson Practice Focus product through a single identification and/or password code being made available to multiple users on a network; or (v) attempt or permit any person without valid identification and/or password codes to attempt to access the McKesson Practice Focus product.
- (g) Client acknowledges (i) that certain services or obligations of Service Provider hereunder may be dependent on Client providing access to certain data, information, or assistance to Service Provider from time to time (collectively, "Cooperation"); and (ii) that such Cooperation may be essential to the performance of services by Service Provider. The parties agree that any delay or failure by Service Provider to provide Services hereunder which is caused by Client's failure to provide timely Cooperation reasonably requested by Service Provider shall not be deemed to be a breach of Service Provider's performance obligations under this MA.
- (h) Client acknowledges that (i) the McKesson Practice Focus product embodies valuable and proprietary trade secrets of Service Provider, (ii) the identification and password codes issued by Service Provider hereunder constitute valuable confidential information, which is proprietary to Service Provider, (iii) the McKesson Practice Focus product may be utilized by Client only to facilitate its use of the Services hereunder in accordance with the terms of this MA, (iv) any reports, report formats, documents, ideas or other discoveries made or developed by Client during its use of the McKesson Practice Focus product may be utilized by Client only to facilitate its use of the Services hereunder in accordance with the terms of this MA and shall not be given or sold to or used on behalf of any third-party and shall remain the sole and exclusive property of Service Provider, and (v) Client agrees, and will cause its employees, agents, subcontractors and representatives to agree, that it/they shall not copy, modify, change, disassemble, or reverse engineer any part or aspect of the McKesson Practice Focus product. Client shall safeguard the right to access the McKesson Practice Focus product and confidentiality of such identification and password codes, using the same standard of care which Client uses for its similar confidential materials, but in no event less than reasonable care.
- (i) Client acknowledges and agrees that it is solely responsible for the security of any information received through McKesson Practice Focus on any device or in any printed format.



**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
Contract Number: RMS153968  
SAP Customer Number:

- (j) Client acknowledges and agrees that it shall timely notify Service Provider of any Authorized User Client no longer wishes to have access to the Software.

**3. SERVICE FEES**

- 3.1. Beginning on the Commencement Date listed in Section 1 above, Client agrees to pay Service Provider the fees as set forth below:
- 3.1.1. User Access. Service Provider will provide 3 Authorized Users at no cost to Client for Intermediate User Access; and
  - 3.1.2. Training Services. If Client's Manager request private classes at a Service Provider facility or at Client's site, the parties will agree to the terms in a separate amendment to this MA; and
  - 3.1.3. Consulting Services. If Client's Manager request Consulting Services, the parties will agree to the terms in a separate amendment to this MA; and
  - 3.1.4. eLearning Training for Intermediate User Access. If Client's Manager request eLearning Training for Intermediate User Access, then Service Provider will provide a 1 year subscription at an amount equal to \$250.00 per year per Authorized User. If Client has signed up for Live Intermediate Training (either on-site or off-site), eLearning Training will be provided at no cost to Client; and
  - 3.1.5. Mobile Electronic Authorized User Access. If Client's Manager request Mobile electronic access McKesson Practice Focus by means of an I-Pad or other mobile electronic device, the parties will agree to the terms in a separate amendment to this MA.

CONFIDENTIAL AND PROPRIETARY

Client: Basha Diagnostics  
 Contract Number: RMS153968  
 SAP Customer Number:

## EXHIBIT E

<b>McKESSON</b>	Client Name
Please complete ALL tabs within this workbook. For Questions below, please list your answers in column B of this spreadsheet. If a question does not apply please enter N/A in the space under column B. For Documents, please provide the file name of the attachment for the requested document under column B.	
<b>Documents</b>	<b>Attachment File Name(s)</b>
Copy of Signed W-9 with Lockbox Address	
Copy of Group letterhead	
Copy of Client Logo (Black and White)	
Endorsement Stamp (if applicable)	
Group Medicare Provider Number (and copy of Welcome Letter)	
Group Medicaid Provider Number (and copy of Welcome Letter)	
Copy of Medicare 855R - Reassignment of Benefits	
<b>Client Days and Hours of operation</b>	<b>Response(s)</b>
Authorized Signer (Medicare and Medicaid)	
Authorized Delegated Official (Medicare and Medicaid)	
Authorized Signer (Commercial Payers)	
Services in a HPSA area? (CM checks if unknown to client)	
Facility FOHC (Federally Qualified Health Center)?	
Specified date that Month End Reports must be delivered by:	
<b>Copies of CMS 1500 Claim forms and UB04 (if applicable), for all Providers</b>	
Provide copies of Lab Requisition forms that are currently in use	
Provide accession wheels (used in Lab billing)	
List of EDI / ERA Payers	
List of Payers paid via EFT - Electronic Funds Transfer	
Identification of any carve-outs	
Provide a listing of capitated Payers	
Copies of Patient Statements	
Provide copies of most frequently used patient letters that are sent out of	
<b>Outreach / Locations that have special billing requirements and special processing (perhaps manual demographics and charge capture, teen outreach, mobile services)</b>	<b>Response(s)</b>
Any programs that require special handling that may present patient privacy issues (teen programs, HIV, genetic counseling, VIP)	
Do you have any special billing arrangements or programs (such as with sports team, correctional facilities, grants, DME, encounter billing, sliding scale) that require special handling?	
If yes, please populate details as indicated below, multiple special	
<b>Terms of programs and grants</b>	
Effective dates	
Contacts, internal and external	
Participating departments	
Participating doctors, by department	
Fee structure	
Reimbursement rate	
Billing address	
Telephone number	
File Claim forms or Invoice (list bill)?	
Define billing cycle (daily, weekly, monthly, etc.)	

**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
 Contract Number: RMS153968  
 SAP Customer Number:

<b>MCKESSON</b>	Client Name
Do you use Case Rates for transplants, etc.?	
How will the process be handled?	
Will there be carve out for research?	
How will the billing be processed if grants are involved?	
Nursing Home Clients? (Lab clients only):	
Mileage Billing Requirements (Lab clients only):	
Census Report Details (Lab clients only):	
<b>Document(s)</b>	<b>Attachment File Name(s)</b>
Small Balance Write Off Amount? Dollar value of small balance is set at	
Debit balance amount? Debit balances only apply to Governmental. Non	
Governmental can apply to both credit and debit. Dollar value of small	
Copy of Financial Assistance / Charity Care policies with associated schedules	
Copy of Deceased Write Off policy	
Copy of self-pay, copay and direct-pay policies and procedures	
Do you extend prompt pay discounts? If yes, indicate maximum discount amount and terms.	
Please have Client complete "DISCOUNT ARRANGEMENT"	
Copy of employee discounts to be applied and indicator to identify these	
Copy of policy for billing non-par patient balances	
Does the client provide services to patients in states that have some form of balance billing prohibitions for patient services? (i.e. New York, Maryland, California etc.) CM is to review the PHYSN_CMPL_Balance Billing Prohibition policy "state by state" chart to ensure all processes required for that given state have been reviewed/implemented. CLIENT CANNOT BE PROVIDED A COPY	
Patient Balance Budget Plans: Minimum payments/over what time period	
Copy of Bankruptcy policy	
Returned checks - NSF Policy and charges to be applied to patient	
Copy of state and out of state Medicaid policies	
List of Insurance company proposed settlements and / or projects	
Copy of any policies and procedures for determining contractual adjustments and allowables for bad debt	
Will charges be captured/provided where BPS will enter as Non-Billable	
<b>Document(s)</b>	<b>Attachment File Name(s)</b>
Does the client currently have a Compliance Program/Policies, to include	
Is the client currently under a corporate integrity agreement with the OIG or	
any other entity? If yes, please obtain a copy and forward to CPD	
Need copy of existing coding workflow and procedures	
Provide samples of all reports for which MCK will be performing coding services (for coding/billing review) and forward to Coding Manager	
Provide copy of final report (must contain acceptable signature as defined by CMS)	
Copy of dictations / procedure notes	
Secure copy of face sheet (paper sites) / registration from each site	
Compile copy of all standing orders / according to protocol utilized by	

**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
 Contract Number: RMS153968  
 SAP Customer Number:

<b>MCKESSON</b>	Client Name
Compile Provider signature sheet, Performing Physicians, Practitioners	
Copies of Provider Schedules (i.e. Locums, Telerad, etc)	
Does the group participate in PQRS?	
Identify PQRS measures that MCK will be coding for	
Provide copy of authorization letter if coding for Anesthesia Physician Quality Initiative Program (if applicable)	
<b>Company Name</b>	
<b>Contact Name</b>	
<b>Contact Phone</b>	
<b>Contact email address</b>	
<b>Physical address</b>	
<b>Special Instructions for Communication:</b>	

**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
Contract Number: RMS153968  
SAP Customer Number:

**EXHIBIT F**  
**Permitted Off-Shore Subcontractors**

Omega Healthcare Management Services  
AGS Health, Inc.  
Pacific Global, Inc.

These sub-contractors may perform some of the following functions: coding, data entry, remittance processing and reconciliation, payment/adjustment/denial posting and reconciliation, non-patient and non-client facing reimbursement management tasks including but not limited to: denial and edit processing, appeal processing and follow-up, insurance "No Response" workqueues, insurance payment validation, bad mail, and claim attachment submissions.

**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
 Contract Number: RMS153968  
 SAP Customer Number:

**SERVICE SCHEDULE 1  
 SCOPE OF SERVICES – RADIOLOGY**

The MA Terms and Conditions and this Service Schedule apply to all services rendered by Service Provider under this Service Schedule.

**1. TERM**

- 1.1. Initial Term of Schedule. The initial term of this Service Schedule is two years (the "Schedule Term") beginning September 1, 2016 (the "Commencement Date").
- 1.2. Termination. Either party may terminate this Service Schedule at any time following the expiration of the initial Schedule Term upon sixty (60) days prior written notice to the other party.
- 1.3. Automatic Renewal. This Service Schedule will automatically renew for one year terms unless (i) either party delivers to the other written notice of termination at least 90 days prior to the expiration of the then-current term, or (ii) as otherwise set forth in the MA.

**2. SCOPE OF SERVICES**

- 2.1. Scope. Service Provider will provide practice management services as specified below based on information provided by Client for radiology services rendered by Client in accordance with the terms of the MA and this Service Schedule.
- 2.2. Responsibilities. Each party agrees to perform its respective responsibilities identified below in a timely and diligent manner. Client acknowledges and agrees that Service Provider's performance of the Services described herein is dependent upon Client's performance of its responsibilities as set forth in this Service Schedule.

**2.2.1. Service Provider Responsibilities. Service Provider will:**

- (a) Enter demographic information and coding information into the Billing System.
- (b) Receive electronic transfer of demographic data from hospital, where available (may require physician involvement).
- (c) Prepare and submit claims to insurance carriers or to patients directly if no insurance information was provided within twenty four (24) hours after receipt of all information necessary to submit the claims.
- (d) Receive electronic copies of the physician's finalized dictated reports and check for completeness.
- (e) Code each finalized dictated report, on the basis of the information provided by Client, including ICD and CPT codes, procedural modifiers and HCPCS Level II regulatory modifiers.
- (f) Provide a toll-free telephone number to answer telephone inquiries from patients and payers.
- (g) Receive all payment and reimbursement notices for Client and post payments to the appropriate patient account.
- (h) Send statements to patients in Client's name.
- (i) Follow up on denials and unpaid insurance and self-pay accounts.
- (j) Provide monthly management reporting.
- (k) Research, identify, and notify Client of overpayments. Overpayments that remain unresolved 60 days after Client's receipt of notice will be removed from the Billing System upon a five (5) business days' notice to Client.
- (l) Notify Client in writing of the Monthly Refund Amount owed by Client for the previous month. Upon Client's deposit of the Monthly Refund Amount in the Refund Account, prepare, sign and release the applicable individual patient and carrier refund checks.
- (m) Prepare checks for individual patient and carrier refunds for Client's signature and release.



**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
 Contract Number: RMS153968  
 SAP Customer Number:

- (n) If Client requests Service Provider to forward its unpaid billings to a collection agency or law firm chosen by Client ("Collection Agent"), Service Provider will transmit the information required by the Collection Agent either by hard copy or electronically, in a mutually acceptable format, as requested by such Collection Agent, pursuant to instructions provided to Service Provider by Client. If Client chooses not to send its unpaid billings to a Collection Agent, then Client hereby consents to Service Provider's removal of such accounts from the active accounts receivable that would otherwise be eligible to be sent to a Collection Agent as defined by Service Provider's normal business practices.
- (o) If requested by Client, assist Client in recovering its share of funds payable to Client under class action settlement agreements ("Settlement Funds") with insurance carriers, manage care companies or other third party entities (each a "Settlement Party") through a third-party vendor with whom Services Provider works to obtain Settlement Funds ("Settlement Recovery Vendor").
- (p) Provide physician enrollment (and re-enrollment) services provided that Client provides the necessary information and secures the necessary signatures on completed enrollment forms in a timely manner.
- (q) Review Client's fee schedule.
- (r) Review managed care contracts.
- (s) Review charges and provide an analysis including projections.
- (t) If requested by Client, provide annual impact analysis of Medicare changes.

**2.2.2. Client Responsibilities. Client will:**

- (a) Electronically provide information required to perform the Services on a timely and ongoing basis, including charts to support completion of claims, information identified in the implementation process and information required for submission of worker's compensations claims. The information Client provides will include, but not be limited to:
  - (i) patient's name, sex, date of birth and status (single, married, other)
  - (ii) responsible party's (insured's) name (if different from patient), sex, date of birth, address, telephone number, relationship to patient, employer (if group policy) and employer's address
  - (iii) name of insurance company, address, policy certificate number and group policy number
  - (iv) copy of any departmental log where Client service is rendered
  - (v) all applicable charge documents
  - (vi) copy of release of information and insurance assignment of benefits, upon request by Service Provider
  - (vii) HMO/PPO authorization numbers approvals (if applicable)
  - (viii) copy of paid at time of service receipt (if applicable)
  - (ix) date of service, chief complaint, medical history and exam, treatment, final diagnosis and physicians' notes
  - (x) any other information Service Provider requests to perform the Services described herein
- (b) Periodically (but not more often than once per week) send to Service Provider all notices Client receives about payment and reimbursement.
- (c) Obtain a release of information and insurance assignment of benefits from all individuals for whom Client is submitting charges. Immediately notify Service Provider if the release of information and insurance assignment of benefits is changed or revoked or if the individual refused/failed to execute

**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
 Contract Number: RMS153968  
 SAP Customer Number:

- the required documents. Client further agrees to provide a copy of signed documents upon Service Provider's request.
- (d) Send medical records/charts to support completing claims for Services. If medical records are missing or inaccurate or incomplete, they will be identified by Service Provider and Client or hospital staff will locate the missing records or obtain the incomplete or inaccurate data.
  - (e) Establish or require a third-party to establish electronic transmission of patients' demographics and financial information from place of service to Service Provider.
  - (f) Designate one or more members of Client's staff to answer questions regarding claims.
  - (g) Notify Service Provider of patients who qualify for free or reduced charge services due to financial hardship.
  - (h) Provide Client's fee schedule (and update as necessary) for entry onto the Billing System prior to the Commencement Date.
  - (i) Provide Service Provider with an electronic file, if available, of Client's referring physicians, including unique, identifying codes, NPI and license numbers. Provide Service Provider with electronic updates, if available, to the file, containing similar required data, on a minimum monthly basis.
  - (j) Provide Service Provider with copies of contracted agreements with managed care plans, including the negotiated fee schedules.
  - (k) Maintain and fund a separate bank account for refunds due by Client to individual patients and/or carriers (the "Refund Account"). Fund such Refund Account each month in an amount equal to the total refund payments due by Client to individual patients and/or carriers (the "Monthly Refund Amount") within ten business days of Client's receipt of notification from Service Provider of such Monthly Refund Amount owed by Client. Client further authorizes Service Provider, upon Client's deposit of the Monthly Refund Amount in the Refund Account, to prepare, sign and release the applicable individual patient and carrier refund checks. However, if Client has not funded the Refund Account so that the posted balance exceeds the total refund amount by ten business days after notification by Service Provider, Client must prepare, sign, and release the refund check(s) on its own behalf despite Client having selected this option.
  - (l) Send refunds of all overpayments in a timely manner.
  - (m) If Client contracts with a physician not under the employ of Client to provide services for Client, and such physician cannot reassign its benefits to Client, Client will notify Service Provider prior to such physician beginning to provide services for Client. If Service Provider is to provide the Services for such physician, Client agrees the physician must enter into an agreement for the performance of the Services with Service Provider with respect to such physician's accounts receivable.
  - (n) Be responsible for its unclaimed property and any required documentation (including, but not limited to, Client's unclaimed property return).
  - (o) Provide names, detailed summary information and copies of applicable licenses for physicians for initiation of payer enrollment by Service Provider, secure the necessary signatures on completed enrollment forms in a timely manner and coordinate the timely return of completed and signed physician enrollment applications and electronic claim submission authorization forms for all physicians.
  - (p) If Client asks Service Provider to recover Settlement Funds, Client (i) authorizes Service Provider to coordinate with the Settlement Recovery Vendor to obtain Settlement Funds for Client; (ii) agrees to provide the necessary assistance and sign any authorization or other document reasonably requested by Service Provider, a Settlement Party or the

**CONFIDENTIAL AND PROPRIETARY**

Client: Basha Diagnostics  
 Contract Number: RMS153968  
 SAP Customer Number:

Settlement Recovery Vendor; (iii) acknowledge and agree that Service Provider makes no warranty, representation or promise that it will obtain any specified amount of Settlement Funds; and (iv) acknowledge and agree that once Settlement Recovery Vendor has begun recovery of the Settlement Funds, the fees owed on the Settlement Funds to Service Provider and the Settlement Recovery Vendor are due and payable to those parties even if the MA has terminated for any reason or expired, except where the Client terminated the MA or a Business Associate Addendum for cause.

- (q) If Client requests Service Provider to forward its unpaid billings to a Collection Agent, Client shall: (1) provide Service Provider with written notice of the name and address of the Collection Agent; (2) provide Service Provider with written instructions on which unpaid billings shall be forwarded to such Collection Agent; and (3) if applicable, provide Service Provider with written authorization to execute documents presented to Service Provider and considered necessary for the collection of Client's unpaid billings by such Collection Agent on Client's behalf in accordance with the written instructions of Client. Client acknowledges and agrees (i) that Client is solely responsible for the unpaid billings, once such unpaid billings are placed with such Collection Agent; and (ii) if Client does not engage a Collection Agent, Service Provider will write-off unpaid billings pursuant to Client's normal business practices.

### 3. SERVICE FEES

- 3.1. Beginning on the Commencement Date, Client agrees to pay Service Provider the fees as set forth below:

#### 3.1.1. Percentage of Net Collections.

- (a) For that certain period of time beginning on the Commencement Date and ending six months thereafter, Client agrees to pay Service Provider an amount equal to 3% of the Net Collections (as defined below) made on Client's accounts receivable during the previous month;
- (b) At the beginning of the six month period beginning in the seventh month of the Schedule Term and at the beginning of each three month period thereafter (each such period a "Period"), Service Provider will determine the "Average Yield Per Procedure" (as defined below) made on Client's radiology accounts receivable during the six month period immediately preceding the then-current Period (each such period a "Measurement Period"), and the fee percentage for the then-current Period shall be an amount equal to a percentage of the Net Collections made on Client's radiology accounts receivable during the previous month, such percentage to be determined in accordance with the schedule set forth below:

Average Yield Per Procedure During the Measurement Period	Monthly Fee Percentage for the Then-Current Period
\$199.05 and above	2.55%
\$179.05 to \$199.04	2.75%
\$179.04 and below	3.0%

"Average Yield Per Procedure" for the then-current Period is determined by dividing the Net Collections made on Client's radiology accounts receivable during the immediately preceding Measurement Period by the number of procedures processed by Service Provider during such Measurement Period

**Jasmina Jakupovic**

---

**From:** Pingston, Howard <Howard.Pingston@McKesson.com>  
**Sent:** Friday, June 10, 2016 12:51 PM  
**To:** Jasmina Jakupovic  
**Subject:** RE: Draft and Execution Copy of Basha 6/8

Hi Jasmina/Dr. Basha,

If the agreement is executed today Friday June 10<sup>th</sup>, as per the language in the agreement we will be on the schedule for a September 1<sup>st</sup>, go-live date. The London, KY office will be processing your business.

Thanks,

**Howard Pingston, MHSA**  
Business Development

313-220-9674 Cell Phone  
248-850-7529 Fax

**McKesson**  
Business Performance Services  
[www.mckesson.com](http://www.mckesson.com)

---

**From:** Jasmina Jakupovic [<mailto:jasmina@bashaopenmri.com>]  
**Sent:** Friday, June 10, 2016 12:42 PM  
**To:** Pingston, Howard  
**Cc:** [hpington@gmail.com](mailto:hpington@gmail.com)  
**Subject:** RE: Draft and Execution Copy of Basha 6/8

Hi Howard  
Below is the email from Dr. Basha.

"Now I need to get a commitment in writing For a starting date, and the area of service Station..  
So Jasmina  
Please call Howard .. And see if he can Confirm.  
Yahya Basha.  
Sent from my iPhone"

Jasmina Jakupovic  
**Basha Diagnostics, P.C.**  
30701 Woodward Ave Ste LL  
Royal Oak, MI 48073  
Telephone: 248.288.1600  
Facsimile: 248.288.1409  
Mobile: 248.837.5868  
[jasmina@bashaopenmri.com](mailto:jasmina@bashaopenmri.com)

This email message and any accompanying data or files is confidential and may contain privileged information intended only for the named recipient(s). If you are not the intended recipient(s), you are hereby notified that the dissemination, distribution, and/or copying of this message is strictly prohibited. If you receive this message in error, or are not the named recipient(s), please notify the sender at the email address above, delete this email from your computer, and destroy any copies in any form immediately. Receipt by anyone other than the named recipients(s) is not a waiver of any attorney-client work product, or other applicable privilege.

## TRANSMISSION VERIFICATION REPORT

TIME : 06/10/2016 15:16  
 NAME : BASHA BNK RO LL  
 FAX : 12482882171  
 TEL : 12482881600  
 SER.# : 000J1N979913

DATE, TIME 06/10 15:02  
 FAX NO./NAME 912488507529  
 DURATION 00:13:38  
 PAGE(S) 33  
 RESULT OK  
 MODE STANDARD

## CONFIDENTIAL AND PROPRIETARY

Client: Basha Diagnostics  
 Contract Number: RMS153968

## MASTER SERVICES AGREEMENT

This MASTER SERVICES AGREEMENT (this "MA") is effective the latest date in the signature block below (the "Effective Date") between PST Services, Inc. ("Service Provider") and Basha Diagnostics, P.C. ("Client"), consisting of the MA Terms and Conditions and all Exhibits, Schedules, and Amendments. This MA governs all the Services described on a Service Schedule that is included in this MA during the term.

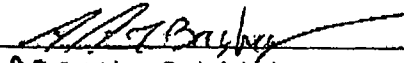
Subject to the terms and conditions of this MA, Client agrees to purchase from Service Provider, and Service Provider agrees to provide Client with, the service(s) listed in the table below (individually, a "Service" and collectively, the "Services"). The description of each Service provided under this MA and any additional terms and conditions relating to such Service are set forth in the Service Schedule referenced in the table below and attached hereto.

Service Schedule	
Radiology	Service Schedule 1
McKesson Practice Focus Web Based Reporting	Service Schedule 2

This MA is executed by an authorized representative of each party.

## BASHA DIAGNOSTICS, P.C.

## PST SERVICES, INC.

By:   
 Printed Name: ABDUL BASHA  
 Title: MANAGER  
 Date: 6/10/16  
 Tax ID: 38-2753824

By: \_\_\_\_\_  
 Printed Name: \_\_\_\_\_  
 Title: \_\_\_\_\_  
 Date: \_\_\_\_\_

Client:  
 30701 Woodward Avenue  
 Royal Oak, Michigan 48073  
 Attention: \_\_\_\_\_

Service Provider:  
 5995 Windward Parkway  
 Alpharetta, Georgia 30005  
 Attention: President

With a copy to the General Counsel at the same address

yes ☐  
 no ☐

invoices sent to above address

# ***EXHIBIT 2***



Advertisement

SECURITY

## UnitedHealth confirms ransomware gang behind Change Healthcare hack amid ongoing pharmacy outages

Ransomware gang ALPHV/BlackCat claims huge breach of US patient records

Zack Whittaker

7:15 AM PST · February 29, 2024

IMAGE CREDITS: PATRICK T. FALLON / AFP / GETTY IMAGES

American health insurance giant UnitedHealth Group has confirmed a ransomware attack on its health tech subsidiary Change Healthcare, which continues to disrupt hospitals and pharmacies across the United States.

“Change Healthcare can confirm we are experiencing a cyber security issue perpetrated by a cybercrime threat actor who has represented itself to us as ALPHV/Blackcat,” said Tyler Mason, vice president at UnitedHealth, in a statement to TechCrunch on Thursday.

“Our experts are working to address the matter and we are working closely with law enforcement and leading third-party consultants,

Mandiant and Palo Alto Network[s], on this attack against Change Healthcare's systems. We are actively working to understand the impact to members, patients and customers," the spokesperson said.

"Based on our ongoing investigation, there's no indication that except for the Change Healthcare systems, Optum, UnitedHealthcare and UnitedHealth Group systems have been affected by this issue."

Advertisement

In a post on its dark web leak site on Wednesday, ALPHV/BlackCat took credit for the cyberattack at Change Healthcare. The Russia-based ransomware and extortion gang claimed to have stolen millions of Americans' sensitive health and patient information. Ransomware gangs typically publish the names of their victims to their dark web leak sites often as a way to extort the victims into paying a ransom demand.

ALPHV/BlackCat's claims could not be immediately verified. ALPHV took down the post claiming responsibility, sometimes an indication that the victim is negotiating with the hackers. UHG spokesperson Mason did not respond to a comment asking if the company paid a ransom or is in negotiations with the hackers.

TechCrunch confirmed on Monday that the ongoing cyberattack was linked to ransomware. Reuters first reported the news.

TC

**TechCrunch Disrupt 2025**  
**Disrupt 2025 will be here before you know it!**  
**Secure your ticket now at the lowest price of the year. From AI and startups to space, fintech, and IPOs—experience game-changing insights across five main stages, breakouts, roundtables, unparalleled networking, and so much more.**

San Francisco, CA | October 27-29

REGISTER NOW

Latest Security  
Startups AI  
Venture Apps  
Apple DOGE

Sign In

Events  
Podcasts

## Newsletters

with benefit plans and another five million outside of the United States, according to [its latest full-year earnings report](#). Optum serves about 103 million U.S. customers.

## Pharmacy outages stall prescriptions

The cyberattack [began on February 21](#) early on the U.S. East Coast, causing widespread outages at pharmacies and healthcare facilities. Change Healthcare said it took much of its systems offline to expel the hackers from its systems.

Change Healthcare's [incident tracker page](#) shows most of its customer-facing systems remain offline.

## Advertisement

Hospitals, healthcare providers and pharmacies across the United States have reported that they are unable to fulfill or process prescriptions through patients' insurance.

Nebraska television outlet [KLKN-TV reports that the majority of Nebraska hospitals](#) are unable to verify patient insurance for inpatient stays, provide precise cost estimates, or process patient billing as a result of the ongoing cyberattack at Change Healthcare.

U.S. military health insurance provider Tricare said [in a statement this week](#) that the cyberattack at Change Healthcare is "impacting all military pharmacies worldwide and some retail pharmacies nationally."

UnitedHealth [previously attributed the cyberattack to an unspecified nation-state actor](#). Researchers have yet to determine a link between the ALPHV/BlackCat group and a government.

"The ransomware problem has been getting worse for years. If governments don't get it under control quickly, critical services will continue to be disrupted, with potentially catastrophic consequences," said Brett Callow, a ransomware expert and threat analyst at Emsisoft, told TechCrunch.

It's not yet clear how the hackers gained access to Change Healthcare's systems. In an interview with TechCrunch on Thursday, ConnectWise chief information security officer Patrick Beggs ruled out a recent vulnerability in his company's products as the cause of the cyberattack at Change Healthcare.

"With all the subsidiaries including United all the way down to Change Healthcare, we have no record or no indication of any [managed service provider supporting them, or them themselves having ScreenConnect installed on their infrastructure," Beggs told TechCrunch.

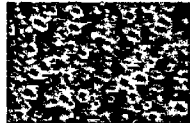
UnitedHealth made \$22 billion in profit during 2023, according to its full-year earnings filed in January. According to the company's most recent report on executive pay, UnitedHealth's chief executive Andrew Witty received close to \$21 million in total compensation during the previous fiscal year.

Advertisement

*TechCrunch's Carly Page contributed reporting.*

*Do you work at Change Healthcare, Optum or UnitedHealth and know more about the cyberattack? Get in touch on Signal and WhatsApp at +1 646-755-8849, or by email. You can also send files and documents via SecureDrop.*

### US health tech giant Change Healthcare hit by cyberattack



U.S. healthcare technology giant Change Healthcare has confirmed a cyberattack on its systems. In a brief statement Wednesday, the company said it was "experiencing a network interruption related to a cyber security issue." "Once we became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to ... Continue

reading

Topics: [Biotech & Health](#) [cyberattack](#) [cybersecurity](#) [Exclusive](#) [healthcare](#)

[Optum](#) [Security](#) [U.S. government](#) [UnitedHealth](#)



**Zack Whittaker**  
Security Editor

Zack Whittaker is the security editor at TechCrunch. You can send tips securely via Signal and WhatsApp to +1 646-755-8849. He can also be reached by email at [zack.whittaker@techcrunch.com](mailto:zack.whittaker@techcrunch.com). You can also submit files and documents securely via [SecureDrop](#).

[View Bio](#) >

FORBES > BUSINESS

**BREAKING**

# Change Healthcare Blames 'Blackcat' Group For Cyber Attack That Disrupted Pharmacies And Health Systems

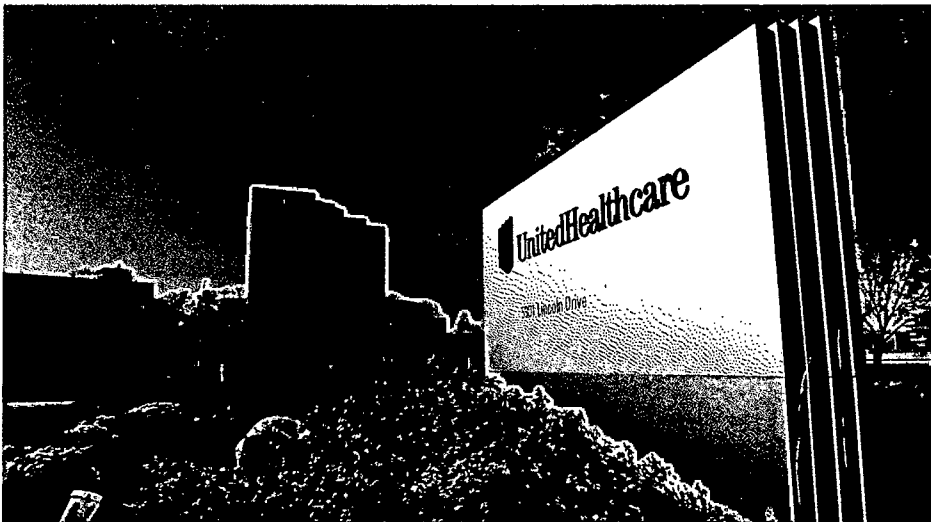
**James Farrell** Former Staff

*James Farrell is a breaking news reporter on the Forbes news team.*



Feb 29, 2024, 01:18pm EST

**TOPLINE** UnitedHealth-owned Change Healthcare has confirmed the ransomware group “ALPHV/Blackcat” is behind its recent cyber attack, after initially suspecting a “nation-state associated cyber security threat actor,” as disruptions to pharmacies continue nearly a week after the attack was reported.



FILE - A sign stands on UnitedHealth Group Inc.'s campus in Minnetonka, Minn., on Oct. 16, 2012. ... [+] COPYRIGHT 2022 THE ASSOCIATED PRESS. ALL RIGHTS RESERVED.

## KEY FACTS

- Change Healthcare said Blackcat was behind the attack and the company is still “working to understand the impact to members, patients and customers.”
- The company also says it’s working with law enforcement and cybersecurity companies Mandiant and Palo Alto Networks to address the cyber attack, which is ongoing.
- While UnitedHealth initially blamed a “nation-state” in a filing last week, cybersecurity experts say Blackcat has no known affiliations with any government—cybersecurity analyst Brett Callow told Reuters “as far as I am aware, they are financially motivated cybercriminals and nothing more.”
- The group reportedly posted about the attack on the dark web, claiming it had accessed “more than 6 TB of highly selective data,” including medical and dental records,

payment information and patients' private information from a variety of Change Healthcare partners, though some reports say the post has since been deleted.

- Change Healthcare's systems remain down since the Feb. 21 attack, causing continued disruptions to pharmacies and other health systems.

#### WHO IS BLACKCAT?

Blackcat—also known as ALPHV or Noverus—typically follows a “ransomware-as-a-service” model, where developers create ransomware and affiliates use the ransomware to identify and attack “high-value victim institutions,” according to a December release from the Department of Justice. The DOJ says Blackcat typically steals victims' data and then encrypts it, blocking them from accessing it. The group then charges a ransom in exchange for releasing the data and not publishing it. The Justice Department says Blackcat has triggered hundreds of millions of dollars worth of losses worldwide.

#### KEY BACKGROUND

Following the attack on Feb. 21, UnitedHealth shut down Change Healthcare's system. The company said it believes the issue has only impacted Change Healthcare and “all other systems across UnitedHealth Group are operational.” Numerous pharmacies, including CVS, Walgreens, Publix and GoodRX, reported some level of business disruption related to the cyber attack.

#### TANGENT

The Wall Street Journal reported Tuesday the Department of Justice had launched an antitrust investigation into UnitedHealth. In 2022, the Department tried to block United subsidiary Optum's merger with Change Healthcare, but failed, allowing for Change Healthcare to become part of Optum and UnitedHealth.

#### FURTHER READING

FORBES

#### Change Healthcare Cyberattack Disrupts Services Nationwide-Here's What To Know

By Molly Bohannon

*Follow me on Twitter. Send me a secure tip.*



James Farrell

James Farrell is a reporter who covers breaking news, often focusing on international affairs, cybersecurity and criminal justice. He... [Read More](#)

Editorial Standards

Forbes Accolades

ADVERTISEMENT



**Optum**Solution Status

[Subscribe to Updates](#)

For further updates about the Change Healthcare cybersecurity issue, please visit [Change Healthcare Cyber Response](#).  
For imaging solutions, please visit us at [Change Healthcare Enterprise Imaging](#).

**Update: restoration in progress of  
Change Healthcare products and  
services. Hover or tap here for  
previous updates.**

**Incident Report for Optum Solutions**

<b>Resolved</b>	<p>This incident has been resolved.</p> <p>Posted 10 months ago. May 07, 2024 - 09:23 EDT</p>
<b>Update</b>	<p>UnitedHealth Group continues to make progress in mitigating the impact to consumers and care providers of the unprecedented cyberattack on the U.S. health system and the Change Healthcare services. Updates on restoration activities and additional resources are available at <a href="#">Information on the Change Healthcare Cyber Response</a>.</p> <p>You can also join our <a href="#">Community</a> for additional support references or view the <a href="#">current payer lists</a>.</p> <p>Real-time Change Healthcare product status updates can be found on the <a href="#">Optum Solutions Status page</a>.</p> <p>Posted 10 months ago. May 07, 2024 - 09:22 EDT</p>
<b>Update</b>	<p>Change Healthcare and Optum are working together to restore products and services, beginning with medical network and transaction services such as Pharmacy solutions, Exchange clearinghouse, Assurance Reimbursement Management, Clearance Patient Access Suite and Reimbursement Manager as well as claims and eligibility transactions. <a href="#">Learn more</a>. When you see green checkmarks next to your products or services, please contact your client manager or use your normal support channels for assistance reconnecting. You can also join our <a href="#">Community</a> for additional support references or view the <a href="#">current payer list</a>. We are continuing with restoration activities daily and additional restorations will be updated here as available.</p> <p>Posted 10 months ago. Apr 23, 2024 - 10:44 EDT</p>
<b>Update</b>	<p>Change Healthcare and Optum are working together to restore products and services, beginning with medical network and transaction services such as Pharmacy solutions, Exchange clearinghouse, Assurance Reimbursement Management, Clearance Patient Access Suite and Reimbursement Manager</p>

as well as claims and eligibility transactions. Learn more. When you see green checkmarks next to your products or services, please contact your client manager or use your normal support channels for assistance reconnecting. You can also join our Community for additional support references or view the current payer list. We are continuing with restoration activities daily and additional restorations will be updated here as available.

Posted 11 months ago. Apr 05, 2024 - 15:55 EDT

#### Update

Change Healthcare and Optum are working together to restore products and services, beginning with medical network and transaction services such as Pharmacy solutions, Exchange clearinghouse, Assurance Reimbursement Management, Clearance Patient Access Suite and Reimbursement Manager as well as claims and eligibility transactions. Learn more. When you see green checkmarks next to your products or services, please contact your client manager or use your normal support channels for assistance reconnecting. You can also join our Community for additional support references or view the current payer list. We are continuing with restoration activities daily and additional restorations will be updated here as available.

Posted 11 months ago. Mar 31, 2024 - 15:03 EDT

#### Update

Assurance Reimbursement Management is currently processing batch claims. Please contact your client manager or use your normal support channels for assistance reconnecting. We are continuing with restoration activities daily. Additional functionality will be updated here as they are made available. View the current payer list.

We have completed standing up a new instance of Change Healthcare's Rx CardFinder Service in a new environment. Testing was successful with Surescripts and Relay Health on both commercial and TROOP queries. As a result, we are enabling this service for all customers effective 6 p.m. CT, Friday, March 15.

We are working to restore access for providers that lost claims and ERA connectivity during the Change Healthcare cybersecurity issue. Over the next several weeks, Optum is working with government payers and intermediaries to transition providers enrolled in Change Healthcare connections to the Optum IEDI Clearinghouse (Exchange claims and ERAs, Change Healthcare OKC Clearinghouse claims and ERAs, Assurance Reimbursement Management, Revenue Performance Advisor). This transition includes both claims and ERA transactions. Our payers will maintain dual enrollment for claims to ensure an easy transition as our platforms come online. Partners and providers do not need to take any action. This transition is ongoing; please allow us and the payers time to complete this effort. We will publish additional updates as they are available.

We are pleased to share that we have launched a new instance of the Rx Connect (Switch) service and are actively working to restore full service and connectivity claim traffic. As a result, we have begun enabling Rx Connect, Rx Edit, and Rx Assist services today, March 7th. These services are now

available for customers who have configured direct internet access connectivity.

For further updates about the Change Healthcare cybersecurity issue, please visit <https://www.unitedhealthgroup.com/changehealthcarecyberresponse>.

Change Healthcare will use this solution status page to provide updates about specific products and services, including uptime and support availability. We are working on multiple approaches to continue to restore the impacted environments.

Posted 11 months ago. Mar 28, 2024 - 10:26 EDT

#### Update

We have completed standing up a new instance of Change Healthcare's Rx CardFinder Service in a new environment. Testing was successful with Surescripts and Relay Health on both commercial and TROOP queries. As a result, we are enabling this service for all customers effective 6 p.m. CT, Friday, March 15.

We are working to restore access for providers that lost claims and ERA connectivity during the Change Healthcare cybersecurity issue. Over the next several weeks, Optum is working with government payers and intermediaries to transition providers enrolled in Change Healthcare connections to the Optum iEDI Clearinghouse (Exchange claims and ERAs, Change Healthcare OKC Clearinghouse claims and ERAs, Assurance Reimbursement Management, Revenue Performance Advisor). This transition includes both claims and ERA transactions. Our payers will maintain dual enrollment for claims to ensure an easy transition as our platforms come online. Partners and providers do not need to take any action. This transition is ongoing; please allow us and the payers time to complete this effort. We will publish additional updates as they are available.

We are pleased to share that we have launched a new instance of the Rx Connect (Switch) service and are actively working to restore full service and connectivity claim traffic. As a result, we have begun enabling Rx Connect, Rx Edit, and Rx Assist services today, March 7th. These services are now available for customers who have configured direct internet access connectivity.

For further updates about the Change Healthcare cybersecurity issue, please visit <https://www.unitedhealthgroup.com/changehealthcarecyberresponse>.

Change Healthcare will use this solution status page to provide updates about specific products and services, including uptime and support availability. We are working on multiple approaches to continue to restore the impacted environments.

Posted 11 months ago. Mar 11, 2024 - 17:51 EDT

#### Update

We are pleased to share that we have launched a new instance of the Rx Connect (Switch) service and are actively working to restore full service and connectivity claim traffic. As a result, we have begun enabling Rx Connect, Rx Edit, and Rx Assist services today, March 7th. These services are now available for customers who have configured direct internet

access connectivity.

For further updates about the Change Healthcare cybersecurity issue, please visit <https://www.unitedhealthgroup.com/changehealthcarecyberresponse>.

Change Healthcare will use this solution status page to provide updates about specific products and services, including uptime and support availability. We are working on multiple approaches to continue to restore the impacted environments.

Posted 1 year ago. Mar 07, 2024 - 18:09 EST

#### Update

For further updates about the Change Healthcare cybersecurity issue, please visit <https://www.unitedhealthgroup.com/changehealthcarecyberresponse>.

Change Healthcare will use this solution status page to provide updates about specific products and services, including uptime and support availability. We are working on multiple approaches to continue to restore the impacted environments.

Posted 1 year ago. Mar 04, 2024 - 12:17 EST

#### Update

Change Healthcare can confirm we are experiencing a cybersecurity issue perpetrated by a cybercrime threat actor who has represented itself to us as ALPHV/Blackcat.

Our experts are working to address the matter and we are working closely with law enforcement and leading third-party consultants, Mandiant and Palo Alto Network, on this attack against Change Healthcare's systems. We are actively working to understand the impact to members, patients and customers.

Patient care is our top priority, and we have multiple workarounds to ensure people have access to the medications and the care they need. Based on our ongoing investigation, there's no indication that Optum, UnitedHealthcare and UnitedHealth Group systems have been affected by this issue.

We are working on multiple approaches to restore the impacted environment and continue to be proactive and aggressive with all our systems, and if we suspect any issue with the system, we will immediately take action.

Posted 1 year ago. Mar 02, 2024 - 09:08 EST

#### Update

We have completed standing up a new instance of Change Healthcare's Rx ePrescribing service. (*Clinical Exchange ePrescribing* providers' tools are still not operational.) Working with technology and business partners, we have successfully completed testing with vendors and multiple retail pharmacy partners for the impacted transaction types. As a result, we have enabled this service for all customers effective 1 p.m. CT, Friday, March 1, 2024. If you encounter issues following the activation of this script routing service, contact our support team through your normal channels or submit an online ticket via our support portal.

Posted 1 year ago. Mar 01, 2024 - 15:40 EST

#### Update

We have completed standing up a new instance of Change Healthcare's Rx ePrescribing service. Working with technology and business partners, we have successfully completed testing

with vendors and multiple retail pharmacy partners for the impacted transaction types. As a result, we have enabled this service for all customers effective 1 p.m. CT, Friday, March 1, 2024. If you encounter issues following the activation of this script routing service, contact our support team through your normal channels or submit an online ticket via our support portal.

Posted 1 year ago. Mar 01, 2024 - 15:03 EST

#### Update

Change Healthcare can confirm we are experiencing a cybersecurity issue perpetrated by a cybercrime threat actor who has represented itself to us as ALPHV/Blackcat.

Our experts are working to address the matter and we are working closely with law enforcement and leading third-party consultants, Mandiant and Palo Alto Network, on this attack against Change Healthcare's systems. We are actively working to understand the impact to members, patients and customers.

Patient care is our top priority, and we have multiple workarounds to ensure people have access to the medications and the care they need. Based on our ongoing investigation, there's no indication that Optum, UnitedHealthcare and UnitedHealth Group systems have been affected by this issue.

We are working on multiple approaches to restore the impacted environment and continue to be proactive and aggressive with all our systems, and if we suspect any issue with the system, we will immediately take action.

Posted 1 year ago. Mar 01, 2024 - 09:17 EST

#### Update

Change Healthcare can confirm we are experiencing a cybersecurity issue perpetrated by a cybercrime threat actor who has represented itself to us as ALPHV/Blackcat.

Our experts are working to address the matter and we are working closely with law enforcement and leading third-party consultants, Mandiant and Palo Alto Network, on this attack against Change Healthcare's systems. We are actively working to understand the impact to members, patients and customers.

Patient care is our top priority, and we have multiple workarounds to ensure people have access to the medications and the care they need. Based on our ongoing investigation, there's no indication that Optum, UnitedHealthcare and UnitedHealth Group systems have been affected by this issue.

We are working on multiple approaches to restored the impacted environment and continue to be proactive and aggressive with all our systems, and if we suspect any issue with the system, we will immediately take action.

Posted 1 year ago. Feb 29, 2024 - 10:50 EST

#### Update

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, and in the interest of protecting our partners and patients, we took immediate action to disconnect Change Healthcare's systems to prevent further impact. This action was taken so our customers and partners do not need to. We have a high-level of confidence that

Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue.

We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 28, 2024 - 17:58 EST

#### **Update**

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, and in the interest of protecting our partners and patients, we took immediate action to disconnect Change Healthcare's systems to prevent further impact. This action was taken so our customers and partners do not need to. We have a high-level of confidence that Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue.

We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 28, 2024 - 10:46 EST

#### **Update**

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, and in the interest of protecting our partners and patients, we took immediate action to disconnect Change Healthcare's systems to prevent further impact. This action was taken so our customers and partners do not need to. We have a high-level of confidence that Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue.

We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 28, 2024 - 08:07 EST

#### **Update**

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, and in the interest of protecting our partners and patients, we took immediate action to disconnect Change Healthcare's systems to prevent further impact. This action was taken so our customers and partners do not need to. We have a high-level of confidence that



Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue.

We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 27, 2024 - 18:53 EST

#### Update

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, and in the interest of protecting our partners and patients, we took immediate action to disconnect Change Healthcare's systems to prevent further impact. This action was taken so our customers and partners do not need to. We have a high-level of confidence that Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue.

We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 27, 2024 - 18:02 EST

#### Update

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, and in the interest of protecting our partners and patients, we took immediate action to disconnect Change Healthcare's systems to prevent further impact. This action was taken so our customers and partners do not need to. We have a high-level of confidence that Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue.

We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 27, 2024 - 14:29 EST

#### Update

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, and in the interest of protecting our partners and patients, we took immediate action to disconnect Change Healthcare's systems to prevent further impact. This action was taken so our customers and partners do not need to. We have a high-level of confidence that

Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue.

We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 27, 2024 - 09:03 EST

#### Update

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, and in the interest of protecting our partners and patients, we took immediate action to disconnect Change Healthcare's systems to prevent further impact. This action was taken so our customers and partners do not need to. We have a high-level of confidence that Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue.

We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 26, 2024 - 22:04 EST

#### Update

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, and in the interest of protecting our partners and patients, we took immediate action to disconnect Change Healthcare's systems to prevent further impact. This action was taken so our customers and partners do not need to. We have a high-level of confidence that Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue.

We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 26, 2024 - 18:11 EST

#### Update

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, and in the interest of protecting our partners and patients, we took immediate action to disconnect Change Healthcare's systems to prevent further impact. This action was taken so our customers and partners do not need to. We have a high-level of confidence that

Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue.

We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 26, 2024 - 14:02 EST

#### Update

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, and in the interest of protecting our partners and patients, we took immediate action to disconnect Change Healthcare's systems to prevent further impact. This action was taken so our customers and partners do not need to. We have a high-level of confidence that Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue.

We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 26, 2024 - 08:04 EST

#### Update

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, and in the interest of protecting our partners and patients, we took immediate action to disconnect Change Healthcare's systems to prevent further impact. This action was taken so our customers and partners do not need to. We have a high-level of confidence that Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue.

We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 25, 2024 - 21:55 EST

#### Update

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, and in the interest of protecting our partners and patients, we took immediate action to disconnect Change Healthcare's systems to prevent further impact. This action was taken so our customers and partners do not need to. We have a high-level of confidence that

Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue.

We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 25, 2024 - 18:03 EST

#### Update

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, and in the interest of protecting our partners and patients, we took immediate action to disconnect Change Healthcare's systems to prevent further impact. This action was taken so our customers and partners do not need to. We have a high-level of confidence that Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue.

We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 25, 2024 - 13:57 EST

#### Update

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, and in the interest of protecting our partners and patients, we took immediate action to disconnect Change Healthcare's systems to prevent further impact. This action was taken so our customers and partners do not need to. We have a high-level of confidence that Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue.

We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 25, 2024 - 08:04 EST

#### Update

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, and in the interest of protecting our partners and patients, we took immediate action to disconnect Change Healthcare's systems to prevent further impact. This action was taken so our customers and partners do not need to. We have a high-level of confidence that

Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue.

We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 24, 2024 - 22:02 EST

#### Update

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, and in the interest of protecting our partners and patients, we took immediate action to disconnect Change Healthcare's systems to prevent further impact. This action was taken so our customers and partners do not need to. We have a high-level of confidence that Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue.

We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 24, 2024 - 18:03 EST

#### Update

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, and in the interest of protecting our partners and patients, we took immediate action to disconnect Change Healthcare's systems to prevent further impact. This action was taken so our customers and partners do not need to. We have a high-level of confidence that Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue.

We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 24, 2024 - 14:06 EST

#### Update

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, and in the interest of protecting our partners and patients, we took immediate action to disconnect Change Healthcare's systems to prevent further impact. This action was taken so our customers and partners do not need to. We have a high-level of confidence that

Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue.

We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 24, 2024 - 08:03 EST

#### **Update**

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, and in the interest of protecting our partners and patients, we took immediate action to disconnect Change Healthcare's systems to prevent further impact. This action was taken so our customers and partners do not need to. We have a high-level of confidence that Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue.

We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 23, 2024 - 22:43 EST

#### **Update**

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, and in the interest of protecting our partners and patients, we took immediate action to disconnect Change Healthcare's systems to prevent further impact. This action was taken so our customers and partners do not need to. We have a high-level of confidence that Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue.

We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 23, 2024 - 18:32 EST

#### **Update**

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, and in the interest of protecting our partners and patients, we took immediate action to disconnect Change Healthcare's systems to prevent further impact. This action was taken so our customers and partners do not need to. We have a high-level of confidence that



Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue.

We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 23, 2024 - 18:20 EST

#### Update

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, and in the interest of protecting our partners and patients, we took immediate action to disconnect Change Healthcare's systems to prevent further impact. This action was taken so our customers and partners do not need to. We have a high-level of confidence that Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue.

We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 23, 2024 - 18:03 EST

#### Update

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, and in the interest of protecting our partners and patients, we took immediate action to disconnect Change Healthcare's systems to prevent further impact. This action was taken so our customers and partners do not need to. We have a high-level of confidence that Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue.

We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 23, 2024 - 14:20 EST

#### Update

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to disconnect our systems to prevent further impact. At this time, we believe the issue is specific to Change Healthcare and all other systems across UnitedHealth Group are

operational. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 23, 2024 - 09:54 EST

**Update**

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to disconnect our systems to prevent further impact. At this time, we believe the issue is specific to Change Healthcare and all other systems across UnitedHealth Group are operational. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 23, 2024 - 08:02 EST

**Update**

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to disconnect our systems to prevent further impact. At this time, we believe the issue is specific to Change Healthcare and all other systems across UnitedHealth Group are operational. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 22, 2024 - 22:05 EST

**Update**

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to disconnect our systems to prevent further impact. At this time, we believe the issue is specific to Change Healthcare and all other systems across UnitedHealth Group are operational. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 22, 2024 - 18:28 EST

**Update**

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to disconnect our systems to prevent further impact. At this time, we believe the issue is specific to Change Healthcare and all other systems across UnitedHealth Group are operational. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 22, 2024 - 15:42 EST

**Update**

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to disconnect our systems to prevent further impact. At this time, we believe the issue is specific to Change Healthcare and all other systems across UnitedHealth Group are

operational. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 22, 2024 - 15:41 EST

**Update**

Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter. Once we became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to disconnect our systems to prevent further impact. At this time, we believe the issue is specific to Change Healthcare and all other systems across UnitedHealth Group are operational. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 22, 2024 - 11:32 EST

**Update**

Change Healthcare is experiencing a network interruption related to a cyber security issue and our experts are working to address the matter. Once we became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to disconnect our systems to prevent further impact. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 22, 2024 - 10:47 EST

**Update**

Change Healthcare is experiencing a network interruption related to a cyber security issue and our experts are working to address the matter. Once we became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to disconnect our systems to prevent further impact. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 22, 2024 - 09:09 EST

**Update**

Change Healthcare is experiencing a network interruption related to a cyber security issue and our experts are working to address the matter. Once we became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to disconnect our systems to prevent further impact. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 22, 2024 - 07:57 EST

**Update**

Change Healthcare is experiencing a network interruption related to a cyber security issue and our experts are working to address the matter. Once we became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to disconnect our systems to prevent further impact. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 22, 2024 - 05:52 EST

**Update**

Change Healthcare is experiencing a network interruption related to a cyber security issue and our experts are working to address the matter. Once we became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to disconnect our systems to

prevent further impact. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 22, 2024 - 01:01 EST

**Update**

Change Healthcare is experiencing a network interruption related to a cyber security issue and our experts are working to address the matter. Once we became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to disconnect our systems to prevent further impact. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 21, 2024 - 23:00 EST

**Update**

Change Healthcare is experiencing a network interruption related to a cyber security issue and our experts are working to address the matter. Once we became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to disconnect our systems to prevent further impact. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 21, 2024 - 22:59 EST

**Update**

Change Healthcare is experiencing a network interruption related to a cyber security issue and our experts are working to address the matter. Once we became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to disconnect our systems to prevent further impact. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 21, 2024 - 20:57 EST

**Update**

Change Healthcare is experiencing a network interruption related to a cyber security issue and our experts are working to address the matter. Once we became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to disconnect our systems to prevent further impact. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 21, 2024 - 18:32 EST

**Update**

Change Healthcare is experiencing a network interruption related to a cyber security issue and our experts are working to address the matter. Once we became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to disconnect our systems to prevent further impact. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 21, 2024 - 17:11 EST

**Update**

Change Healthcare is experiencing a network interruption related to a cyber security issue and our experts are working to address the matter. Once we became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to disconnect our systems to

prevent further impact. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 21, 2024 - 16:27 EST

**Update** Change Healthcare is experiencing a network interruption related to a cyber security issue and our security experts are working to address the matter. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.

Posted 1 year ago. Feb 21, 2024 - 14:09 EST

**Update** We are experiencing a network interruption and are working to resolve the issue. The disruption is expected to last at least through the day. We will update you as soon as we have more information.

Posted 1 year ago. Feb 21, 2024 - 10:18 EST

**Update** We are experiencing a network interruption and are working to resolve the issue. The disruption is expected to last at least through the day. We will update you as soon as we have more information.

Posted 1 year ago. Feb 21, 2024 - 09:55 EST

**Update** We are currently experiencing enterprise-wide connectivity issues. We are actively isolating and troubleshooting the issue. Please follow the Optum Solution status page for ongoing updates at

<https://status.changehealthcare.com/incidents/hqpjz25fn3n7>.

Posted 1 year ago. Feb 21, 2024 - 09:43 EST

**Update** We are currently experiencing enterprise-wide connectivity issues. We are actively isolating and troubleshooting the issue. Please follow the Optum Solution status page for ongoing updates at

<https://status.changehealthcare.com/incidents/hqpjz25fn3n7>.

Posted 1 year ago. Feb 21, 2024 - 09:11 EST

**Update** We are currently experiencing enterprise-wide connectivity issues. We are actively isolating and troubleshooting the issue. Please follow the Optum Solution status page for ongoing updates at

<https://status.changehealthcare.com/incidents/hqpjz25fn3n7>.

Posted 1 year ago. Feb 21, 2024 - 08:41 EST

**Update** We are currently experiencing enterprise-wide connectivity issues. We are actively isolating and troubleshooting the issue.

Posted 1 year ago. Feb 21, 2024 - 08:38 EST

**Update** Update: We are experiencing connectivity issues and support teams are actively troubleshooting to resolve them.

INC/CSA/Ref # 0529634

Posted 1 year ago. Feb 21, 2024 - 07:39 EST

**Update** Update: Some applications are currently unavailable. Optum is currently triaging the issue and will provide further updates as they are available. We apologize for the inconvenience that this situation has caused you.

INC/CSA/Ref # 0529634

Posted 1 year ago. Feb 21, 2024 - 06:48 EST

**Update** We are currently experiencing enterprise-wide connectivity issues. We are actively isolating and troubleshooting the issue.  
Posted 1 year ago. Feb 21, 2024 - 06:10 EST

**Update** We are currently experiencing enterprise-wide connectivity issues. We are actively isolating and troubleshooting the issue.  
Posted 1 year ago. Feb 21, 2024 - 06:01 EST

**Update** Update: Feb. 21, 2024, some applications are currently unavailable. Optum is currently triaging the issue and will provide further updates as they are available. We apologize for the inconvenience that this situation has caused you.

INC/CSA/Ref # 0529634

Posted 1 year ago. Feb 21, 2024 - 05:52 EST

**Update** We are currently experiencing enterprise-wide connectivity issues. We are actively isolating and troubleshooting the issue.  
Posted 1 year ago. Feb 21, 2024 - 05:44 EST

**Update** We are currently experiencing enterprise-wide connectivity issues. We are actively isolating and troubleshooting the issue.  
Posted 1 year ago. Feb 21, 2024 - 05:05 EST

**Identified** Feb. 21, 2024, some applications are currently unavailable. Optum is currently triaging the issue and will provide further updates as they are available. We apologize for the inconvenience that this situation has caused you.

INC/CSA/Ref # 0529634

Posted 1 year ago. Feb 21, 2024 - 02:15 EST

This Incident affected: Change Healthcare Enterprise, Cost Transparency (Predictive Engagement, Provider Directory), Medical Network Services (eligibility, enrollment and clearinghouse) (Advanced Claim Management, Remittance/ERA transmission, Hosted Payer Services (HPS), Medical claim attachments, Payer Connectivity Services, Revenue Analytics), Medical Record Retrieval & Clinical Review (Clinical Abstraction, Medical Record Retrieval), Patient Engagement & Experience (Shop Book and Pay, Virtual Front Desk), Provider Network Optimization (Contract Manager, Provider Manager), Revenue Cycle Management (AccuPost, Acuity Revenue Cycle Analytics, Ahi Lobby, AhiQA, Ambulatory Claims Manager, Claims & Denials Advisor, Claims & Denials Management, Clearance Patient Access Suite, Financial Clearance Services, National Payments Connector, Patient Engagement Suite, Revenue Integrity (Coding Services), Revenue Performance Advisor), Value-Based Care (Business Process as a Service (BPaaS), HealthQx, Prometheus Analytics, Risk Manager, Third-Party Administration), Customer Portals (Client Access System, ConnectCenter, Customer Care Hub, Enrollment Central), Payment Integrity (DRG Validation, Hospital Bill Audit, Hospital Billing Validation/Short Stay Bill Validation), Dental Network (Dental Claim Attachments, Dental Converge, Dental Credentialing Manager, Dental EDI Network, Dental Practice Analytic Insights, Dental Revenue Cycle Insights), Government Eligibility, Enrollment & Member Engagement (Smart Connect, Smart Appointment Scheduling, & Clinical Care Visits), Clinical Network (Clinical Exchange Channel Partners including ePrescribe and Orders & Results, Clinical Exchange Labs and Hospitals), Payer Communications and Payment Services (Payer Enrollment Services), Provider Communications and Payment Services (Payment Automation), Risk Adjustment & Quality (Risk View, Risk Adjustment Coding), Medical Network APIs (Payer Finder website and API), Pharmacy Solutions (MedRx), and Clinical Decision Support (InterQual® Review Manager – Hosted, InterQual® Government Services).



**Company**

[About us](#)

[Newsroom](#)

**Support**

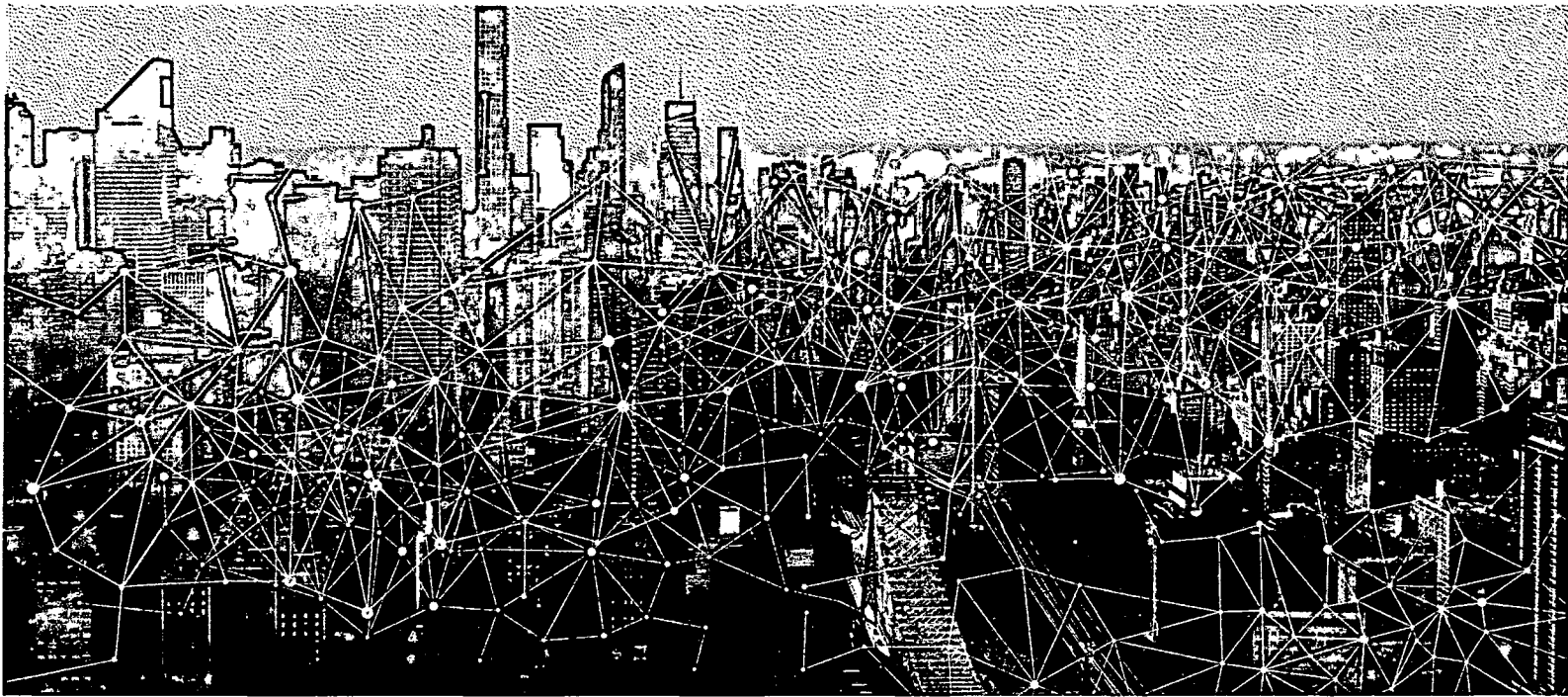
[Customer support](#)

[Customer Care Hub](#)

[Change Healthcare](#)

[Community](#)

**TLP:WHITE**



# **JOINT CYBERSECURITY ADVISORY**

---

## **Ransomware Activity Targeting the Healthcare and Public Health Sector**

AA20-302A

October 28, 2020

*Updated October 29, 2020*



**TLP:WHITE**

**JOINT  
CYBERSECURITY ADVISORY**

CISA | FBI | HHS

**TLP:WHITE**

**Note:** This advisory was updated on October 29, 2020 to include information on Conti, TrickBot, and BazarLoader, including new IOCs and Yara Rules for detection.

*This advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) version 7 framework. See the [ATT&CK for Enterprise version 7](#) for all referenced threat actor tactics and techniques.*

**SUMMARY**

This joint cybersecurity advisory was coauthored by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS). This advisory describes the tactics, techniques, and procedures (TTPs) used by cybercriminals against targets in the Healthcare and Public Health Sector (HPH) to infect systems with ransomware, notably Ryuk and Conti, for financial gain.

CISA, FBI, and HHS have credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers. CISA, FBI, and HHS are sharing this information to provide warning to healthcare providers to ensure that they take timely and reasonable precautions to protect their networks from these threats.

**Key Findings**

- CISA, FBI, and HHS assess malicious cyber actors are targeting the HPH Sector with TrickBot and BazarLoader malware, often leading to ransomware attacks, data theft, and the disruption of healthcare services.
- These issues will be particularly challenging for organizations within the COVID-19 pandemic; therefore, administrators will need to balance this risk when determining their cybersecurity investments.

**TECHNICAL DETAILS****Threat Details**

The cybercriminal enterprise behind TrickBot, which is likely also the creator of BazarLoader malware, has continued to develop new functionality and tools, increasing the ease, speed, and profitability of victimization. These threat actors increasingly use loaders—like TrickBot and BazarLoader (or BazarBackdoor)—as part of their malicious cyber campaigns. Cybercriminals

---

*To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at [www.fbi.gov/contact-us/field](http://www.fbi.gov/contact-us/field), or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at [CyWatch@fbi.gov](mailto:CyWatch@fbi.gov). When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at [central@cisa.gov](mailto:central@cisa.gov).*

*This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see <http://www.us-cert.gov/tlp/>.*

**TLP:WHITE**

# CYBERSECURITY ADVISORY

**TLP:WHITE**

disseminate TrickBot and BazarLoader via phishing campaigns that contain either links to malicious websites that host the malware or attachments with the malware. Loaders start the infection chain by distributing the payload; they deploy and execute the backdoor from the C2 server and install it on the victim's machine.

## TrickBot

What began as a banking trojan and descendant of Dyre malware, TrickBot now provides its operators a full suite of tools to conduct a myriad of illegal cyber activities. These activities include credential harvesting, mail exfiltration, cryptomining, point-of-sale data exfiltration, and the deployment of ransomware, such as Ryuk and Conti.

In early 2019, FBI began to observe new TrickBot modules named Anchor, which cyber actors typically used in attacks targeting high-profile victims—such as large corporations. These attacks often involved data exfiltration from networks and point-of-sale devices. As part of the new Anchor toolset, TrickBot developers created `anchor_dns`, a tool for sending and receiving data from victim machines using Domain Name System (DNS) tunneling.

`anchor_dns` is a backdoor that allows victim machines to communicate with command and control (C2) servers over DNS to evade typical network defense products and make their malicious communications blend in with legitimate DNS traffic. `anchor_dns` uses a single-byte XOR cipher to encrypt its communications, which have been observed using key `0xB9`. Once decrypted, the string `anchor_dns` can be found in the DNS request traffic.

## TrickBot Indicators of Compromise

After successful execution of the malware, TrickBot copies itself as an executable file with a 12-character (includes `.exe`), randomly generated file name (e.g. `mfjdieks.exe`) and places this file in one of the following directories.

- C:\Windows\
- C:\Windows\SysWOW64\
- C:\Users\[Username]\AppData\Roaming\

Once the executable is running and successful in establishing communication with C2s, the executable places appropriate modules downloaded from C2s for the infected processor architecture type (32 or 64 bit instruction set), to the infected host's `%APPDATA%` or `%PROGRAMDATA%` directory, such as `%AppData%\Roaming\winapp`. Some commonly named plugins that are created in a `Modules` subdirectory are (the detected architecture is appended to the module filename, e.g., `importDll32` or `importDll64`):

- `Systeminfo`
- `importDll`
- `outlookDll`
- `injectDll` with a directory (ex. `injectDLL64_configs`) containing configuration files:
  - `dinj`
  - `sinj`

JOINT  
CYBERSECURITY ADVISORY

CISA | FBI | HHS

TLP:WHITE

- dpost
- mailsearcher with a directory (ex. mailsearcher64\_configs) containing configuration file:
  - mailconf
- networkDll with a directory (ex. networkDll64\_configs) containing configuration file:
  - dpost
- wormDll
- tabDll
- shareDll

Filename client\_id or data or FAQ with the assigned bot ID of the compromised system is created in the malware directory. Filename group\_tag or Readme.md containing the TrickBot campaign IDs is created in the malware directory.

The malware may also drop a file named anchorDiag.txt in one of the directories listed above.

Part of the initial network communications with the C2 server involves sending information about the victim machine such as its computer name/hostname, operating system version, and build via a base64-encoded GUID. The GUID is composed of /GroupID/ClientID/ with the following naming convention:

/anchor\_dns/[COMPUTERNAME].[WindowsVersionBuildNo].[32CharacterString]/.

The malware uses scheduled tasks that run every 15 minutes to ensure persistence on the victim machine. The scheduled task typically uses the following naming convention.

[random\_folder\_name\_in\_%APPDATA%\_excluding\_Microsoft]  
autoupdate#[5\_random\_numbers] (e.g., Task autoupdate#16876).

After successful execution, anchor\_dns further deploys malicious batch scripts (.bat) using PowerShell commands.

The malware deploys self-deletion techniques by executing the following commands.

- cmd.exe /c timeout 3 && del C:\Users\[username]\[malware\_sample]
- cmd.exe /C PowerShell - "Start-Sleep 3; Remove-Item C:\Users\[username]\[malware\_sample\_location]"

The following domains found in outbound DNS records are associated with anchor\_dns.

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

This malware used the following legitimate domains to test internet connectivity.

- [REDACTED]
- [REDACTED]

TLP:WHITE

# JOINT CYBERSECURITY ADVISORY

CISA | FBI | HHS

TLP:WHITE

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Currently, there is an open source tracker for Trickbot C2 servers located at <https://feodotracker.abuse.ch/browse/trickbot/>.

The `anchor_dns` malware historically used the following C2 servers.

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

## TrickBot YARA Rules

```
rule anchor_dns_strings_filenames {
  meta:
    description = "Rule to detect AnchorDNS samples based off strings or
  filenames used in malware"
    author = "NCSC"
    hash1 = "fc0efd612ad528795472e99cae5944b68b8e26dc"
    hash2 = "794eb3a9ce8b7e5092bb1b93341a54097f5b78a9"
    hash3 = "9dfce70fded4f3bc2aa50ca772b0f9094b7b1fb2"
    hash4 = "24d4bbc982a6a561f0426a683b9617de1a96a74a"
  strings:
    $ = ";Control_RunDLL \x00"
    $ = ":%GUID" ascii wide
    $ = ":%DATA" ascii wide
    $ = "/1001/"
    $ = /(\\x00|\\xCC)qwertyuiopasdfghjklzxcvbnm(\\x00|\\xCC)/
    $ = /(\\x00|\\xCC)QWERTYUIOPASDFGHJKLZXCVBNM(\\x00|\\xCC)/
```

TLP:WHITE



JOINT  
**CYBERSECURITY ADVISORY**

CISA | FBI | HHS

**TLP:WHITE**

```

$ = "start program with cmdline \"%s\""
$ = "Global\\fde345tyhoVGyHUIJKIOuy"
$ = "ChardWorker::thExecute: error registry me"
$ = "get command: incode %s, cmdid \"%s\", cmd \"%s\""
$ = "anchorDNS"
$ = "Anchor_x86"
$ = "Anchor_x64"

condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and 3 of them
}

rule anchor_dns_icmp_transport {
    meta:
        description = "Rule to detect AnchorDNS samples based off ICMP transport strings"
        author = "NCSC"
        hash1 = "056f326d9ab960ed02356b34a6dcd72d7180fc83"
    strings:
        $ = "reset_connection <- %s"
        $ = "server_ok <- %s (packets on server %s)"
        $ = "erase successfully transmitted packet (count: %d)"
        $ = "Packet sended with crc %s -> %s"
        $ = "send data confimation to server(%s)"
        $ = "data recived from <- %s"
        $ = "Rearmost packed recived (id: %s)"
        $ = "send poll to server -> : %s"
    condition:
        (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and 3 of them
}

```

**TLP:WHITE**

JOINT  
**CYBERSECURITY ADVISORY**

CISA | FBI | HHS

**TLP:WHITE**

```

rule anchor_dns_config_dexor {
    meta:
        description = "Rule to detect AnchorDNS samples based off configuration
deobfuscation (XOR 0x23 countup)"
        author = "NCSC"
        hash1 = "d0278ec015e10ada000915a1943ddbb3a0b6b3db"
        hash2 = "056f326d9ab960ed02356b34a6dcd72d7180fc83"
    strings:
        $x86 = {75 1F 56 6A 40 B2 23 33 C9 5E 8A 81 ?? ?? ?? ?? 32 C2 FE C2 88 81
?? ?? ?? ?? 41 83 EE 01 75 EA 5E B8 ?? ?? ?? ?? C3}
        $x64 = {41 B0 23 41 B9 80 00 00 00 8A 84 3A ?? ?? ?? 00 41 32 C0 41 FE C0
88 04 32 48 FF C2 49 83 E9 01 75 E7}
    condition:
        (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and any of them
}

rule anchor_dns_installer {
    meta:
        description = "Rule to detect AnchorDNS installer samples based off MZ
magic under one-time pad or deobfuscation loop code"
        author = "NCSC"
        hash1 = "fa98074dc18ad7e2d357b5d168c00a91256d87d1"
        hash2 = "78f0737d2b1e605aad62af252b246ef390521f02"
    strings:
        $pre = {43 00 4F 00 4E 00 4F 00 55 00 54 00 24 00 00 00} //CONOUT$
        $pst = {6B 65 72 6E 65 6C 33 32 2E 64 6C 6C 00 00 00 00} //kernel32.dll
        $deob_x86 = {8B C8 89 4D F8 83 F9 FF 74 52 46 89 5D F4 88 5D FF 85 F6 74
34 8A 83 ?? ?? ?? ?? 32 83 ?? ?? ?? ?? 6A 00 88 45 FF 8D 45 F4 50 6A 01 8D 45 FF
50 51 FF 15 34 80 41 00 8B 4D F8 43 8B F0 81 FB 00 ?? ?? ?? 72 CC 85 F6 75 08}
        $deob_x64 = {42 0F B6 84 3F ?? ?? ?? ?? 4C 8D 8C 24 80 00 00 00 42 32 84
3F ?? ?? ?? ?? 48 8D 54 24 78 41 B8 01 00 00 00 88 44 24 78 48 8B CE 48 89 6C 24
20 FF 15 ?? ?? ?? ?? 48 FF C7 8B D8 48 81 FF ?? ?? ?? ?? 72 B8}

```

**TLP:WHITE**

JOINT  
CYBERSECURITY ADVISORY

CISA | FBI | HHS

TLP:WHITE

```

condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550)
    and
    (    uint16(@pre+16) ^ uint16(@pre+16+((@pst-(@pre+16))\2)) == 0x5A4D
      or
      $deob_x86 or $deob_x64
    )
}

import "pe"

rule anchor_dns_string_1001_with_pe_section_dll_export_resolve_ip_domains {
    meta:
        description = "Rule to detect AnchorDNS samples based off /1001/ string
in combination with DLL export name string, PE section .addr or IP resolution
domains"

        author = "NCSC"

        hash1 = "ff8237252d53200c132dd742edc77a6c67565eee"
        hash2 = "c8299aadf886da55cb47e5cbafe8c5a482b47fc8"

    strings:
        $str1001 = {2F 31 30 30 31 2F 00} // /1001/
        $strCtrl = {2C 43 6F 6E 74 72 6F 6C 5F 52 75 6E 44 4C 20 00} //
,Control_RunDLL

        $ip1 = "checkip.amazonaws.com" ascii wide
        $ip2 = "ipecho.net" ascii wide
        $ip3 = "ipinfo.io" ascii wide
        $ip4 = "api.ipify.org" ascii wide
        $ip5 = "icanhazip.com" ascii wide
        $ip6 = "myexternalip.com" ascii wide
        $ip7 = "wtfismyip.com" ascii wide
        $ip8 = "ip.anysrc.net" ascii wide

    condition:

```

TLP:WHITE

JOINT

**CYBERSECURITY ADVISORY****TLP:WHITE**

CISA | FBI | HHS

```

(uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550)
and $str1001
and (
    for any i in (0..pe.number_of_sections): (
        pe.sections[i].name == ".addr"
    )
or
    $strCtrl
or
    6 of ($ip*)
)
}

rule anchor_dns_check_random_string_in_dns_response {
    meta:
        description = "Rule to detect AnchorDNS samples based off checking random
string in DNS response"
        author = "NCSC"
        hash1 = "056f326d9ab960ed02356b34a6dcd72d7180fc83"
        hash2 = "14e9d68bba7a184863667c680a8d5a757149aa36"
    strings:
        $x86 = {8A D8 83 C4 10 84 DB 75 08 8B 7D BC E9 84 00 00 00 8B 7D BC 32 DB
8B C7 33 F6 0F 1F 00 85 C0 74 71 40 6A 2F 50 E8 ?? ?? ?? ?? 46 83 C4 08 83 FE 03
72 EA 85 C0 74 5B 83 7D D4 10 8D 4D C0 8B 75 D0 8D 50 01 0F 43 4D C0 83 EE 04 72
11 8B 02 3B 01 75 10 83 C2 04 83 C1 04 83 EE 04 73 EF 83 FE FC 74 2D 8A 02 3A 01
75 29 83 FE FD 74 22 8A 42 01 3A 41 01 75 1C 83 FE FE 74 15 8A 42 02 3A 41 02 75
0F 83 FE FF 74 08 8A 42 03 3A 41 03 75 02 B3 01 8B 75 B8}

        $x64 = {4C 39 75 EF 74 56 48 8D 45 DF 48 83 7D F7 10 48 0F 43 45 DF 49 8B
FE 48 85 C0 74 40 48 8D 48 01 BA 2F 00 00 00 E8 ?? ?? ?? ?? 49 03 FF 48 83 FF 03
72 E4 48 85 C0 74 24 48 8D 55 1F 48 83 7D 37 10 48 0F 43 55 1F 48 8D 48 01 4C 8B
45 2F E8 ?? ?? ?? ?? 0F B6 DB 85 C0 41 0F 44 DF 49 03 F7 48 8B 55 F7 48 83 FE 05
0F 82 6A FF FF FF}

    condition:

```

**TLP:WHITE**

JOINT  
CYBERSECURITY ADVISORY

CISA | FBI | HHS

TLP:WHITE

```

        (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and any of them
    }

rule anchor_dns_default_result_execute_command {
    meta:
        description = "Rule to detect AnchorDNS samples based off default result
value and executing command"
        author = "NCSC"
        hash1 = "056f326d9ab960ed02356b34a6dcd72d7180fc83"
        hash2 = "14e9d68bba7a184863667c680a8d5a757149aa36"

    strings:
        $x86 = {83 C4 04 3D 80 00 00 00 73 15 8B 04 85 ?? ?? ?? ?? 85 C0 74 0A 8D
4D D8 51 8B CF FF D0 8A D8 84 DB C7 45 A4 0F 00 00 00}
        $x64 = {48 98 B9 E7 03 00 00 48 3D 80 00 00 00 73 1B 48 8D 15 ?? ?? ?? ??
48 8B 04 C2 48 85 C0 74 0B 48 8D 55 90 48 8B CE FF D0 8B C8}

    condition:
        (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and any of them
}

```

```

rule anchor_dns_pdb {
    meta:
        description = "Rule to detect AnchorDNS samples based off partial PDB
paths"
        author = "NCSC"
        hash1 = "f0e575475f33600aede6a1b9a5c14f671cb93b7b"
        hash2 = "1304372bd4cdd877778621aea715f45face93d68"
        hash3 = "e5dc7c8bfa285b61dda1618f0ade9c256be75d1a"
        hash4 = "f96613ac6687f5dbbed13c727fa5d427e94d6128"
        hash5 = "46750d34a3a11dd16727dc622d127717beda4fa2"

    strings:
        $ = ":\MyProjects\secondWork\Anchor\"
}

```

TLP:WHITE

JOINT  
**CYBERSECURITY ADVISORY**

CISA | FBI | HHS

**TLP:WHITE**

```

$ = ":\simsim\anchorDNS"
$ = ":\[JOB]\Anchor\"
$ = ":\Anchor\Win32\Release\Anchor_"
$ = ":\Users\ProFi\Desktop\data\Win32\anchor"

condition:

(uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and any of them
}

```

**BazarLoader/BazarBackdoor**

Beginning in approximately early 2020, actors believed to be associated with Trickbot began using BazarLoader and BazarBackdoor to infect victim networks. The loader and backdoor work closely together to achieve infection and communicate with the same C2 infrastructure. Campaigns using Bazar represent a new technique for cybercriminals to infect and monetize networks and have increasingly led to the deployment of ransomware, including Ryuk. BazarLoader has become one of the most commonly used vectors for ransomware deployment.

Deployment of the BazarLoader malware typically comes from phishing email and contains the following:

- Phishing emails are typically delivered by commercial mass email delivery services. Email received by a victim will contain a link to an actor-controlled Google Drive document or other free online filehosting solutions, typically purporting to be a PDF file.
- This document usually references a failure to create a preview of the document and contains a link to a URL hosting a malware payload in the form of a misnamed or multiple extension file.
- Emails can appear as routine, legitimate business correspondence about customer complaints, hiring decision, or other important tasks that require the attention of the recipient.
- Some email communications have included the recipient's name or employer name in the subject line and/or email body.

Through phishing emails linking users to Google Documents, actors used the below identified file names to install BazarLoader:

- Report-Review26-10.exe
- Review\_Report15-10.exe
- Document\_Print.exe
- Report10-13.exe
- Text\_Report.exe

Bazar activity can be identified by searching the system startup folders and Userinit values under the HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon registry key:

%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\adobe.lnk

**TLP:WHITE**



# JOINT CYBERSECURITY ADVISORY

CISA | FBI | HHS

TLP:WHITE

For a comprehensive list of indicators of compromise regarding the BazarLocker malware, see <https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html>.

## Indicators

In addition to TrickBot and BazarLoader, threat actors are using malware, such as KEGTAP, BEERBOT, SINGLEMALT, and others as they continue to change tactics, techniques, and procedures in their highly dynamic campaign.<sup>1</sup> The following C2 servers are known to be associated with this malicious activity.

- 45[.]148[.]10[.]92
- 170[.]238[.]117[.]187
- 177[.]74[.]232[.]124
- 185[.]68[.]93[.]17
- 203[.]176[.]135[.]102
- 96[.]9[.]73[.]73
- 96[.]9[.]77[.]142
- 37[.]187[.]3[.]176
- 45[.]89[.]127[.]92
- 62[.]108[.]35[.]103
- 91[.]200[.]103[.]242
- 103[.]84[.]238[.]3
- 36[.]89[.]106[.]69
- 103[.]76[.]169[.]213
- 36[.]91[.]87[.]227
- 105[.]163[.]17[.]83
- 185[.]117[.]73[.]163
- 5[.]2[.]78[.]118
- 185[.]90[.]61[.]69
- 185[.]90[.]61[.]62
- 86[.]104[.]194[.]30
- 31[.]131[.]21[.]184
- 46[.]28[.]64[.]8
- 104[.]161[.]32[.]111
- 107[.]172[.]140[.]171
- 131[.]153[.]22[.]148
- 195[.]123[.]240[.]219
- 195[.]123[.]242[.]119

<sup>1</sup> FireEye: [Unhappy Hour Special: KEGTAP and SINGLEMALT With a Ransomware Chaser](#)

TLP:WHITE

JOINT  
**CYBERSECURITY ADVISORY**

CISA | FBI | HHS

**TLP:WHITE**

- 195[.]123[.]242[.]120
- 51[.]81[.]113[.]25
- 74[.]222[.]14[.]27

**Ryuk Ransomware**

Typically Ryuk has been deployed as a payload from banking Trojans such as TrickBot.<sup>2</sup> Ryuk first appeared in August 2018 as a derivative of Hermes 2.1 ransomware, which first emerged in late 2017 and was available for sale on the open market as of August 2018. Ryuk still retains some aspects of the Hermes code. For example, all of the files encrypted by Ryuk contain the **HERMES** tag but, in some infections, the files have **Ryuk** added to the filename, while others do not. In other parts of the ransomware code, Ryuk has removed or replaced features of Hermes, such as the restriction against targeting specific Eurasia-based systems.

While negotiating the victim network, Ryuk actors will commonly use commercial off-the-shelf products—such as Cobalt Strike and PowerShell Empire—in order to steal credentials. Both frameworks are very robust and are highly effective dual-purpose tools, allowing actors to dump clear text passwords or hash values from memory with the use of Mimikatz. This allows the actors to inject malicious dynamic-link library into memory with read, write, and execute permissions. In order to maintain persistence in the victim environment, Ryuk actors have been known to use scheduled tasks and service creation.

Ryuk actors will quickly map the network in order to enumerate the environment to understand the scope of the infection. In order to limit suspicious activity and possible detection, the actors choose to live off the land and, if possible, use native tools—such as net view, net computers, and ping—to locate mapped network shares, domain controllers, and active directory. In order to move laterally throughout the network, the group relies on native tools, such as PowerShell, Windows Management Instrumentation (WMI), Windows Remote Management, and Remote Desktop Protocol (RDP). The group also uses third-party tools, such as Bloodhound.

Once dropped, Ryuk uses AES-256 to encrypt files and an RSA public key to encrypt the AES key. The Ryuk dropper drops a **.bat** file that attempts to delete all backup files and Volume Shadow Copies (automatic backup snapshots made by Windows), preventing the victim from recovering encrypted files without the decryption program.

In addition, the attackers will attempt to shut down or uninstall security applications on the victim systems that might prevent the ransomware from executing. Normally this is done via a script, but if that fails, the attackers are capable of manually removing the applications that could stop the attack. The **RyukReadMe** file placed on the system after encryption provides either one or two email

---

<sup>2</sup> See the United Kingdom (UK) National Cyber Security Centre (NCSC) advisory, [Ryuk Ransomware Targeting Organisations Globally](#), on their ongoing investigation into global Ryuk ransomware campaigns and associated Emotet and TrickBot malware.

**TLP:WHITE**

# JOINT CYBERSECURITY ADVISORY

CISA | FBI | HHS

TLP:WHITE

addresses, using the end-to-end encrypted email provider Protonmail, through which the victim can contact the attacker(s). While earlier versions provide a ransom amount in the initial notifications, Ryuk users are now designating a ransom amount only after the victim makes contact.

The victim is told how much to pay to a specified Bitcoin wallet for the decryptor and is provided a sample decryption of two files.

Initial testing indicates that the RyukReadMe file does not need to be present for the decryption script to run successfully but other reporting advises some files will not decrypt properly without it. Even if run correctly, there is no guarantee the decryptor will be effective. This is further complicated because the RyukReadMe file is deleted when the script is finished. This may affect the decryption script unless it is saved and stored in a different location before running.

According to MITRE, Ryuk uses the ATT&CK techniques listed in table 1.

Table 1: Ryuk ATT&CK techniques

Technique	Use
<i>System Network Configuration Discovery [T1016]</i>	Ryuk has called <u>GetIpNetTable</u> in attempt to identify all mounted drives and hosts that have Address Resolution Protocol entries.
<i>Masquerading: Match Legitimate Name or Location [T1036.005]</i>	Ryuk has constructed legitimate appearing installation folder paths by calling <u>GetWindowsDirectoryW</u> and then inserting a null byte at the fourth character of the path. For Windows Vista or higher, the path would appear as <u>C:\Users\Public</u> .
<i>Process Injection [T1055]</i>	Ryuk has injected itself into remote processes to encrypt files using a combination of <u>VirtualAlloc</u> , <u>WriteProcessMemory</u> , and <u>CreateRemoteThread</u> .
<i>Process Discovery [T1057]</i>	Ryuk has called <u>CreateToolhelp32Snapshot</u> to enumerate all running processes.
<i>Command and Scripting Interpreter: Windows Command Shell [T1059.003]</i>	Ryuk has used <u>cmd.exe</u> to create a Registry entry to establish persistence.
<i>File and Directory Discovery [T1083]</i>	Ryuk has called <u>GetLogicalDrives</u> to enumerate all mounted drives, and <u>GetDriveTypeW</u> to determine the drive type.

TLP:WHITE

JOINT  
**CYBERSECURITY ADVISORY**

CISA | FBI | HHS

**TLP:WHITE**

Technique	Use
<i>Native API</i> [T1106]	Ryuk has used multiple native APIs including <code>ShellExecuteW</code> to run executables, <code>GetWindowsDirectoryW</code> to create folders, and <code>VirtualAlloc</code> , <code>WriteProcessMemory</code> , and <code>CreateRemoteThread</code> for process injection.
<i>Access Token Manipulation</i> [T1134]	Ryuk has attempted to adjust its token privileges to have the <code>SeDebugPrivilege</code> .
<i>Data Encrypted for Impact</i> [T1486]	Ryuk has used a combination of symmetric and asymmetric encryption to encrypt files. Files have been encrypted with their own AES key and given a file extension of <code>.RYK</code> . Encrypted directories have had a ransom note of <code>RyukReadMe.txt</code> written to the directory.
<i>Service Stop</i> [T1489]	Ryuk has called <code>kill.bat</code> for stopping services, disabling services and killing processes.
<i>Inhibit System Recovery</i> [T1490]	Ryuk has used <code>vssadmin Delete Shadows /all /quiet</code> to delete volume shadow copies and <code>vssadmin resize shadowstorage</code> to force deletion of shadow copies created by third-party applications.
<i>Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder</i> [T1547.001]	Ryuk has used the Windows command line to create a Registry entry under <code>HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run</code> to establish persistence.
<i>Impair Defenses: Disable or Modify Tools</i> [T1562.001]	Ryuk has stopped services related to anti-virus.

**MITIGATIONS**

For a downloadable copy of IOCs, see [AA20-302A.stix](https://gist.github.com/aaronst/6aa7f61246f53a8dd4bfe86e832456). For additional IOCs detailing this activity, see <https://gist.github.com/aaronst/6aa7f61246f53a8dd4bfe86e832456>.

**Plans and Policies**

CISA, FBI, and HHS encourage HPH Sector organizations to maintain business continuity plans—the practice of executing essential functions through emergencies (e.g., cyberattacks)—to minimize service interruptions. Without planning, provision, and implementation of continuity principles,

**TLP:WHITE**

**JOINT  
CYBERSECURITY ADVISORY**

CISA | FBI | HHS

**TLP:WHITE**

organizations may be unable to continue operations. Evaluating continuity and capability will help identify continuity gaps. Through identifying and addressing these gaps, organizations can establish a viable continuity program that will help keep them functioning during cyberattacks or other emergencies. CISA, FBI, and HHS suggest HPH Sector organizations review or establish patching plans, security policies, user agreements, and business continuity plans to ensure they address current threats posed by malicious cyber actors.

**Network Best Practices**

- Patch operating systems, software, and firmware as soon as manufacturers release updates.
- Check configurations for every operating system version for HPH organization-owned assets to prevent issues from arising that local users are unable to fix due to having local administration disabled.
- Regularly change passwords to network systems and accounts and avoid reusing passwords for different accounts.
- Use multi-factor authentication where possible.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
- Implement application and remote access allow listing to only allow systems to execute programs known and permitted by the established security policy.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Audit logs to ensure new accounts are legitimate.
- Scan for open or listening ports and mediate those that are not needed.
- Identify critical assets such as patient database servers, medical records, and telehealth and telework infrastructure; create backups of these systems and house the backups offline from the network.
- Implement network segmentation. Sensitive data should not reside on the same server and network segment as the email environment.
- Set antivirus and anti-malware solutions to automatically update; conduct regular scans.

**Ransomware Best Practices**

CISA, FBI and HHS do not recommend paying ransoms. Payment does not guarantee files will be recovered. It may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. In addition to implementing the above network best practices, the FBI, CISA and HHS also recommend the following:

- Regularly back up data, air gap, and password protect backup copies offline.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, secure location.

**User Awareness Best Practices****TLP:WHITE**

JOINT

**CYBERSECURITY ADVISORY**

CISA | FBI | HHS

**TLP:WHITE**

- Focus on awareness and training. Because end users are targeted, make employees and stakeholders aware of the threats—such as ransomware and phishing scams—and how they are delivered. Additionally, provide users training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities.
- Ensure that employees know who to contact when they see suspicious activity or when they believe they have been a victim of a cyberattack. This will ensure that the proper established mitigation strategy can be employed quickly and efficiently.

**Recommended Mitigation Measures**

System administrators who have indicators of a TrickBot network compromise should immediately take steps to back up and secure sensitive or proprietary data. TrickBot infections may be indicators of an imminent ransomware attack; system administrators should take steps to secure network devices accordingly. Upon evidence of a TrickBot infection, review DNS logs and use the **XOR** key of **0xB9** to decode **XOR** encoded DNS requests to reveal the presence of **anchor\_dns**, and maintain and provide relevant logs.

**GENERAL RANSOMWARE MITIGATIONS — HPH SECTOR**

*This section is based on CISA and Multi-State Information Sharing and Analysis Center (MS-ISAC)'s Joint Ransomware Guide, which can be found at <https://www.cisa.gov/publication/ransomware-guide>.*

CISA, FBI, and HHS recommend that healthcare organizations implement both ransomware prevention and ransomware response measures immediately.

**Ransomware Prevention****Join and Engage with Cybersecurity Organizations**

CISA, FBI, and HHS recommend that healthcare organizations take the following initial steps:

- Join a healthcare information sharing organization, H-ISAC:
  - Health Information Sharing and Analysis Center (H-ISAC): <https://h-isac.org/membership-account/join-h-isac/>
  - Sector-based ISACs - National Council of ISACs: <https://www.nationalisacs.org/member-isacs>
  - Information Sharing and Analysis Organization (ISAO) Standards Organization: <https://www.isao.org/information-sharing-groups/>
- Engage with CISA and FBI, as well as HHS—through the HHS Health Sector Cybersecurity Coordination Center (HC3)—to build a lasting partnership and collaborate on information sharing, best practices, assessments, and exercises.
  - CISA: [cisa.gov](https://cisa.gov), <https://us-cert.cisa.gov/mailing-lists-and-feeds>, [central@cisa.gov](mailto:central@cisa.gov)
  - FBI: [ic3.gov](https://ic3.gov), [www.fbi.gov/contact-us/field](https://www.fbi.gov/contact-us/field), [CyWatch@fbi.gov](mailto:CyWatch@fbi.gov)
  - HHS/HC3: <http://www.hhs.gov/hc3>, [HC3@HHS.gov](mailto:HC3@HHS.gov)

**TLP:WHITE**



**JOINT  
CYBERSECURITY ADVISORY**

CISA | FBI | HHS

**TLP:WHITE**

Engaging with the H-ISAC, ISAO, CISA, FBI, and HHS/HC3 will enable your organization to receive critical information and access to services to better manage the risk posed by ransomware and other cyber threats.

***Follow Ransomware Best Practices***

Refer to the best practices and references below to help manage the risk posed by ransomware and support your organization's coordinated and efficient response to a ransomware incident. Apply these practices to the greatest extent possible based on availability of organizational resources.

- It is critical to maintain offline, encrypted backups of data and to regularly test your backups. Backup procedures should be conducted on a regular basis. It is important that backups be maintained offline or in separated networks as many ransomware variants attempt to find and delete any accessible backups. Maintaining offline, current backups is most critical because there is no need to pay a ransom for data that is readily accessible to your organization.
  - Use the 3-2-1 rule as a guideline for backup practices. The rule states that three copies of all critical data are retained on at least two different types of media and at least one of them is stored offline.
  - Maintain regularly updated "gold images" of critical systems in the event they need to be rebuilt. This entails maintaining image "templates" that include a preconfigured operating system (OS) and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server.
  - Retain backup hardware to rebuild systems in the event rebuilding the primary system is not preferred.
    - Hardware that is newer or older than the primary system can present installation or compatibility hurdles when rebuilding from images.
    - Ensure all backup hardware is properly patched.
- In addition to system images, applicable source code or executables should be available (stored with backups, escrowed, license agreement to obtain, etc.). It is more efficient to rebuild from system images, but some images will not install on different hardware or platforms correctly; having separate access to needed software will help in these cases.
- Create, maintain, and exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident.
  - Review available incident response guidance, such as CISA's Technical Approaches to Uncovering and Remediating Malicious Activity <https://us-cert.cisa.gov/ncas/alerts/aa20-245a>.
- Help your organization better organize around cyber incident response.
- Develop a cyber incident response plan.
- The Ransomware Response Checklist, available in the [CISA and MS-ISAC Joint Ransomware Guide](#), serves as an adaptable, ransomware- specific annex to organizational cyber incident response or disruption plans.

**TLP:WHITE**

# JOINT CYBERSECURITY ADVISORY

CISA | FBI | HHS

TLP:WHITE

- Review and implement as applicable MITRE's Medical Device Cybersecurity: Regional Incident Preparedness and Response Playbook (<https://www.mitre.org/sites/default/files/publications/pr-18-1550-Medical-Device-Cybersecurity-Playbook.pdf>).
- Develop a risk management plan that maps critical health services and care to the necessary information systems; this will ensure that the incident response plan will contain the proper triage procedures.
- Plan for the possibility of critical information systems being inaccessible for an extended period of time. This should include but not be limited to the following:
  - Print and properly store/protect hard copies of digital information that would be required for critical patient healthcare.
  - Plan for and periodically train staff to handle the re-routing of incoming/existing patients in an expedient manner if information systems were to abruptly and unexpectedly become unavailable.
  - Coordinate the potential for surge support with other healthcare facilities in the greater local area. This should include organizational leadership periodically meeting and collaborating with counterparts in the greater local area to create/update plans for their facilities to both abruptly send and receive a significant amount of critical patients for immediate care. This may include the opportunity to re-route healthcare employees (and possibly some equipment) to provide care along with additional patients.
- Consider the development of a second, air-gapped communications network that can provide a minimum standard of backup support for hospital operations if the primary network becomes unavailable if/when needed.
- Predefine network segments, IT capabilities and other functionality that can either be quickly separated from the greater network or shut down entirely without impacting operations of the rest of the IT infrastructure.
- Legacy devices should be identified and inventoried with highest priority and given special consideration during a ransomware event.
- See CISA and MS-ISAC's Joint Ransomware Guide for infection vectors including internet-facing vulnerabilities and misconfigurations; phishing; precursor malware infection; and third parties and managed service providers.
- HHS/HC3 tracks ransomware that is targeting the HPH Sector; this information can be found at <http://www.hhs.gov/hc3>.

## Hardening Guidance

- The Food and Drug Administration provides multiple guidance documents regarding the hardening of healthcare and specifically medical devices found here: <https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity>.
- See CISA and MS-ISAC's Joint Ransomware Guide for additional in-depth hardening guidance.

TLP:WHITE

# JOINT CYBERSECURITY ADVISORY

TLP:WHITE

CISA | FBI | HHS

## Contact CISA for These No-Cost Resources

- Information sharing with CISA and MS-ISAC (for SLTT organizations) includes bi-directional sharing of best practices and network defense information regarding ransomware trends and variants as well as malware that is a precursor to ransomware.
- Policy-oriented or technical assessments help organizations understand how they can improve their defenses to avoid ransomware infection: <https://www.cisa.gov/cyber-resource-hub>.
  - Assessments include Vulnerability Scanning and Phishing Campaign Assessment.
- Cyber exercises evaluate or help develop a cyber incident response plan in the context of a ransomware incident scenario.
- CISA Cybersecurity Advisors (CSAs) advise on best practices and connect you with CISA resources to manage cyber risk.
- Contacts:
  - SLTT organizations: [CyberLiaison\\_SLTT@cisa.dhs.gov](mailto:CyberLiaison_SLTT@cisa.dhs.gov)
  - Private sector organizations: [CyberLiaison\\_Industry@cisa.dhs.gov](mailto:CyberLiaison_Industry@cisa.dhs.gov)

## Ransomware Quick References

- *Ransomware: What It Is and What to Do About It* (CISA): General ransomware guidance for organizational leadership and more in-depth information for CISOs and technical staff: [https://www.us-cert.cisa.gov/sites/default/files/publications/Ransomware\\_Executive\\_One-Pager\\_and\\_Technical\\_Document-FINAL.pdf](https://www.us-cert.cisa.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf)
- *Ransomware* (CISA): Introduction to ransomware, notable links to CISA products on protecting networks, specific ransomware threats, and other resources: <https://www.us-cert.cisa.gov/Ransomware>
- HHS/HC3: Ransomware that impacts HPH is tracked by the HC3 and can be found at [www.hhs.gov/hc3](http://www.hhs.gov/hc3)
- *Security Primer – Ransomware* (MS-ISAC): Outlines opportunistic and strategic ransomware campaigns, common infection vectors, and best practice recommendations: <https://www.cisecurity.org/white-papers/security-primer-ransomware/>
- *Ransomware: Facts, Threats, and Countermeasures* (MS-ISAC): Facts about ransomware, infection vectors, ransomware capabilities, and how to mitigate the risk of ransomware infection: <https://www.cisecurity.org/blog/ransomware-facts-threats-and-countermeasures/>
- HHS Ransomware Fact Sheet: <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>
- NIST Securing Data Integrity White Paper: <https://csrc.nist.gov/publications/detail/white-paper/2020/10/01/securing-data-integrity-against-ransomware-attacks/draft>

## Ransomware Response Checklist

**Remember: Paying the ransom will not ensure your data is decrypted or that your systems or data will no longer be compromised. CISA, FBI, and HHS do not recommend paying ransom.**

TLP:WHITE

**JOINT  
CYBERSECURITY ADVISORY**

CISA | FBI | HHS

**TLP:WHITE**

Should your organization be a victim of ransomware, CISA strongly recommends responding by using the Ransomware Response Checklist located in CISA and MS-ISAC's Joint Ransomware Guide, which contains steps for detection and analysis as well as containment and eradication.

***Consider the Need For Extended Identification or Analysis***

If extended identification or analysis is needed, CISA, HHS/HC3, or federal law enforcement may be interested in any of the following information that your organization determines it can legally share:

- ☐ Recovered executable file
- ☐ Copies of the readme file – DO NOT REMOVE the file or decryption may not be possible
- ☐ Live memory (RAM) capture from systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally)
- ☐ Images of infected systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally)
- ☐ Malware samples
- ☐ Names of any other malware identified on your system
- ☐ Encrypted file samples
- ☐ Log files (Windows Event Logs from compromised systems, Firewall logs, etc.)
- ☐ Any PowerShell scripts found having executed on the systems
- ☐ Any user accounts created in Active Directory or machines added to the network during the exploitation
- ☐ Email addresses used by the attackers and any associated phishing emails
- ☐ A copy of the ransom note
- ☐ Ransom amount and whether or not the ransom was paid
- ☐ Bitcoin wallets used by the attackers
- ☐ Bitcoin wallets used to pay the ransom (if applicable)
- ☐ Copies of any communications with attackers

Upon voluntary request, CISA can assist with analysis (e.g., phishing emails, storage media, logs, malware) at no cost to support your organization in understanding the root cause of an incident, even in the event additional remote assistance is not requested.

- CISA – Advanced Malware Analysis Center: <https://www.malware.us-cert.gov/MalwareSubmission/pages/submission.jsf>
- Remote Assistance – Request via [Central@cisa.gov](mailto:Central@cisa.gov)

**JOINT  
CYBERSECURITY ADVISORY**

CISA | FBI | HHS

**TLP:WHITE****CONTACT INFORMATION**

CISA, FBI, and HHS recommend identifying and having on hand the following contact information for ready use should your organization become a victim of a ransomware incident. Consider contacting these organizations for mitigation and response assistance or for purpose of notification.

- State and Local Response Contacts
- IT/IT Security Team – Centralized Cyber Incident Reporting
- State and Local Law Enforcement
- Fusion Center
- Managed/Security Service Providers
- Cyber Insurance

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at [www.fbi.gov/contact-us/field](http://www.fbi.gov/contact-us/field), or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at [CyWatch@fbi.gov](mailto:CyWatch@fbi.gov). When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at [Central@cisa.dhs.gov](mailto:Central@cisa.dhs.gov).

Additionally, see [CISA and MS-ISAC's Joint Ransomware Guide](#) for information on contacting—and what to expect from contacting—federal asset response and federal threat response contacts.

**RESOURCES**

- [CISA Emergency Services Sector Continuity Planning Suite](#)
- [CISA MS-ISAC Joint Ransomware Guide](#)
- [CISA Tip: Avoiding Social Engineering and Phishing Attacks](#)
- [FBI PSA: High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations](#)
- [Health Industry Cybersecurity Tactical Crisis Response](#)
- [Health Industry Cybersecurity Practices \(HICP\)](#)
- [HHS - Ransomware Spotlight Webinar](#)
- [HHS - Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients](#)
- [HHS - Ransomware Briefing](#)
- [HHS - Aggressive Ransomware Impacts](#)
- [HHS - Ransomware Fact Sheet](#)
- [HHS - Cyber Attack Checklist](#)
- [HHS - Cyber-Attack Response Infographic](#)
- [NIST - Data Integrity Publication](#)
- [NIST - Guide for Cybersecurity Event Recovery](#)
- [NIST - Identifying and Protecting Assets Against Ransomware and Other Destructive Events](#)
- [NIST - Detecting and Responding to Ransomware and Other Destructive Events](#)
- [NIST - Recovering from Ransomware and Other Destructive Events](#)
- [FireEye - Unhappy Hour Special: KEGTAP and SINGLEMALT With a Ransomware Chaser](#)
- [Github list of IOCs](#)

**TLP:WHITE**

# ***EXHIBIT 5***



# Joint Cybersecurity Advisory TLP Clear:: #StopRansomware: Play Ransomware

🏠 (/) / Data & Insights (/type/data-insights) / Cybersecurity Government Intelligence Reports (/type/cybersecurity-government-intelligence-reports)

December 18, 2023

## SUMMARY

*Note: This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit [stopransomware.gov](https://www.cisa.gov/stopransomware) (<https://www.cisa.gov/stopransomware>) to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.*

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) are releasing this joint CSA to disseminate the Play ransomware group's IOCs and TTPs identified through FBI investigations as recently as October 2023.

Since June 2022, the Play (also known as Playcrypt) ransomware group has impacted a wide range of businesses and critical infrastructure in North America, South America, and Europe. As of October 2023, the FBI was aware of approximately 300 affected entities allegedly exploited by the ransomware actors.

In Australia, the first Play ransomware incident was observed in April 2023, and most recently in November 2023.

The Play ransomware group is presumed to be a closed group, designed to "guarantee the secrecy of deals," according to a statement on the group's data leak website. Play ransomware actors employ a double-extortion model, encrypting systems after exfiltrating data. Ransom notes do not include an initial ransom demand or payment instructions, rather, victims are instructed to contact the threat actors via email.

The FBI, CISA, and ASD's ACSC encourage organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of ransomware incidents. This includes requiring multifactor authentication, maintaining offline backups of data, implementing a recovery plan, and keeping all operating systems, software, and firmware up to date.

### Actions to take today to mitigate cyber threats from Play ransomware:

- Prioritize remediating known exploited vulnerabilities.
- Enable multifactor authentication (MFA) for all services to the extent possible, particularly for webmail, VPN, and accounts that access critical systems.
- Regularly patch and update software and applications to their latest versions and conduct regular vulnerability assessments.

For help with Cybersecurity and Risk Advisory Services exclusively for AHA members, contact:

**John Riggi (/system/files/media/file/2020/11/AHA-Riggi-Senior-Advisor-for-Cyber-and-Risk-Bio-08102020.pdf)**

**National Advisor for Cybersecurity and Risk, AHA**

**[jriggi@aha.org](mailto:jriggi@aha.org) ([mailto:jriggi@aha.org?subject=Cybersecurity and Risk Advisory Services Query](mailto:jriggi@aha.org?subject=Cybersecurity%20and%20Risk%20Advisory%20Services%20Query))**



# JOINT CYBERSECURITY ADVISORY

Co-Authored by:

**TLP:CLEAR**

Product ID: AA23-352A

December 18, 2023



## #StopRansomware: Play Ransomware

### SUMMARY

**Note:** This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit [stopransomware.gov](https://stopransomware.gov) to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.

#### Actions to take today to mitigate cyber threats from Play ransomware:

- Prioritize remediating known exploited vulnerabilities.
- Enable multifactor authentication (MFA) for all services to the extent possible, particularly for webmail, VPN, and accounts that access critical systems.
- Regularly patch and update software and applications to their latest versions and conduct regular vulnerability assessments.

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) are releasing this joint CSA to disseminate the Play ransomware group's IOCs and TTPs identified through FBI investigations as recently as October 2023.

Since June 2022, the Play (also known as Playcrypt) ransomware group has impacted a wide range of businesses and critical infrastructure in North America, South America, and Europe. As of October 2023, the FBI was aware of approximately 300 affected entities allegedly exploited by the ransomware actors.

In Australia, the first Play ransomware incident was observed in April 2023, and most recently in November 2023.

The Play ransomware group is presumed to be a closed group, designed to "guarantee the secrecy of deals," according to a statement on the group's data leak website. Play ransomware actors employ a double-extortion model, encrypting systems after exfiltrating data. Ransom notes do not include an

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at [fbi.gov/contact-us/field-offices](https://fbi.gov/contact-us/field-offices). When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at [Report@cisa.dhs.gov](mailto:Report@cisa.dhs.gov).

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see [cisa.gov/tlp/](https://cisa.gov/tlp/).

**TLP:CLEAR**

JOINT  
**CYBERSECURITY ADVISORY**

FBI | CISA | ACSC

**TLP:CLEAR**

initial ransom demand or payment instructions, rather, victims are instructed to contact the threat actors via email.

The FBI, CISA, and ASD's ACSC encourage organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of ransomware incidents. This includes requiring multifactor authentication, maintaining offline backups of data, implementing a recovery plan, and keeping all operating systems, software, and firmware up to date.

For a downloadable copy of IOCs, see:

- [AA23-352A](#) (STIX XML, 35KB)
- [AA23-352A](#) (STIX JSON, 31KB)

## TECHNICAL DETAILS

**Note:** This advisory uses the MITRE ATT&CK® for Enterprise framework, version 14. See the MITRE ATT&CK for Enterprise section for all referenced tactics and techniques. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

### Initial Access

The Play ransomware group gains initial access to victim networks through the abuse of valid accounts [T1078] and exploitation of public-facing applications [T1190], specifically through known FortiOS (CVE-2018-13379 and CVE-2020-12812) and Microsoft Exchange (ProxyNotShell [CVE-2022-41040 and CVE-2022-41082]) vulnerabilities. Play ransomware actors have been observed to use external-facing services [T1133] such as Remote Desktop Protocol (RDP) and Virtual Private Networks (VPN) for initial access.

### Discovery and Defense Evasion

Play ransomware actors use tools like AdFind to run Active Directory queries [TA0007] and Grixba [1], an information-stealer, to enumerate network information [T1016] and scan for anti-virus software [T1518.001]. Actors also use tools like GMER, IOBit, and PowerTool to disable anti-virus software [T1562.001] and remove log files [T1070.001]. In some instances, cybersecurity researchers have observed Play ransomware actors using PowerShell scripts to target Microsoft Defender.[2]

### Lateral Movement and Execution

Play ransomware actors use command and control (C2) applications, including Cobalt Strike and SystemBC, and tools like PsExec, to assist with lateral movement and file execution. Once established on a network, the ransomware actors search for unsecured credentials [T1552] and use the Mimikatz credential dumper to gain domain administrator access [T1003]. According to open source reporting [2], to further enumerate vulnerabilities, Play ransomware actors use Windows Privilege Escalation Awesome Scripts (WinPEAS) [T1059] to search for additional privilege escalation paths. Actors then distribute executables [T1570] via Group Policy Objects [T1484.001].

**TLP:CLEAR**

JOINT  
**CYBERSECURITY ADVISORY****TLP:CLEAR**

FBI | CISA | ACSC

**Exfiltration and Encryption**

Play ransomware actors often split compromised data into segments and use tools like WinRAR to compress files [T1560.001] into [RAR] format for exfiltration. The actors then use WinSCP to transfer data [T1048] from a compromised network to actor-controlled accounts. Following exfiltration, files are encrypted [T1486] with AES-RSA hybrid encryption using intermittent encryption, encrypting every other file portion of 0x100000 bytes. [3] (**Note:** System files are skipped during the encryption process.) A [play] extension is added to file names and a ransom note titled ReadMe[.]txt is placed in file directory [C:].

**Impact**

The Play ransomware group uses a double-extortion model [T1657], encrypting systems after exfiltrating data. The ransom note directs victims to contact the Play ransomware group at an email address ending in @gmx[.]de. Ransom payments are paid in cryptocurrency to wallet addresses provided by Play actors. If a victim refuses to pay the ransom demand, the ransomware actors threaten to publish exfiltrated data to their leak site on the Tor network ([.onion] URL).

**Leveraged Tools**

Table 1 lists legitimate tools Play ransomware actors have repurposed for their operations. The legitimate tools listed in this product are all publicly available. Use of these tools and applications should not be attributed as malicious without analytical evidence to support they are used at the direction of, or controlled by, threat actors.

*Table 1: Tools Leveraged by Play Ransomware Actors*

Name	Description
AdFind	Used to query and retrieve information from Active Directory.
Bloodhound	Used to query and retrieve information from Active Directory.
GMER	A software tool intended to be used for detecting and removing rootkits.
IOBit	An anti-malware and anti-virus program for the Microsoft Windows operating system. Play actors have accessed IOBit to disable anti-virus software.
Psexec	A tool designed to run programs and execute commands on remote systems.
PowerTool	A Windows utility designed to improve speed, remove bloatware, protect privacy, and eliminate data collection, among other things.
PowerShell	A cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework, which runs on Windows, Linux, and macOS.
Cobalt Strike	A penetration testing tool used by security professionals to test the security of networks and systems. Play ransomware actors have used it to assist with lateral movement and file execution.

**TLP:CLEAR**

JOINT  
**CYBERSECURITY ADVISORY****TLP:CLEAR**

FBI | CISA | ACSC

Name	Description
Mimikatz	Allows users to view and save authentication credentials such as Kerberos tickets. Play ransomware actors have used it to add accounts to domain controllers.
WinPEAS	Used to search for additional privilege escalation paths.
WinRAR	Used to split compromised data into segments and to compress files into <b>RAR</b> format for exfiltration.
WinSCP	Windows Secure Copy is a free and open-source Secure Shell (SSH) File Transfer Protocol, File Transfer Protocol, WebDAV, Amazon S3, and secure copy protocol client. Play ransomware actors have used it to transfer data <b>[T1048]</b> from a compromised network to actor-controlled accounts.
Microsoft Nltest	Used by Play ransomware actors for network discovery.
Nekto / PriviCMD	Used by Play ransomware actors for privilege escalation.
Process Hacker	Used to enumerate running processes on a system.
Plink	Used to establish persistent SSH tunnels.

**Indicators of Compromise**

See Table 2 for Play ransomware IOCs obtained from FBI investigations as of October 2023.

*Table 2: Hashes Associated with Play Ransomware Actors*

Hashes (SHA256)	Description
453257c3494addafb39cb6815862403e827947a1e7737eb8168cd10522465deb	Play ransomware custom data gathering tool
47c7cee3d76106279c4c28ad1de3c833c1ba0a2ec56b0150586c7e8480ccae57	Play ransomware encryptor
75404543de25513b376f097ceb383e8efb9c9b95da8945fd4aa37c7b2f226212	SystemBC malware EXE
7a42f96599df8090cf89d6e3ce4316d24c6c00e499c8557a2e09d61c00c11986	SystemBC malware DLL
7a6df63d883bbccb315986c2cfb76570335abf84fafbefce047d126b32234af8	Play ransomware binary
7dea671be77a2ca5772b86cf8831b02bff0567bce6a3ae023825aa40354f8aca	SystemBC malware DLL

**TLP:CLEAR**

JOINT

**CYBERSECURITY ADVISORY****TLP:CLEAR**

FBI | CISA | ACSC

Hashes (SHA256)	Description
c59f3c8d61d940b56436c14bc148c1fe98862921b8f7bad97fbc96b31d71193c	Play network scanner
e652051fe47d784f6f85dc00adca1c15a8c7a40f1e5772e6a95281d8bf3d5c74	Play ransomware binary
e8d5ad0bf292c42a9185bb1251c7e763d16614c180071b01da742972999b95da	Play ransomware binary

**MITRE ATT&CK TACTICS AND TECHNIQUES**

See Table 3–Table 11 for all referenced threat actor tactics and techniques in this advisory.

*Table 3: Play ATT&CK Techniques for Enterprise for Initial Access*

Technique Title	ID	Use
Valid Accounts	<u>T1078</u>	Play ransomware actors obtain and abuse existing account credentials to gain initial access.
Exploit Public Facing Application	<u>T1190</u>	Play ransomware actors exploit vulnerabilities in internet-facing systems to gain access to networks.
External Remote Services	<u>T1133</u>	Play ransomware actors have used remote access services, such as RDP/VPN connection to gain initial access.

*Table 4: Play ATT&CK Techniques for Enterprise for Discovery*

Technique Title	ID	Use
System Network Configuration Discovery	<u>T1016</u>	Play ransomware actors use tools like Grixba to identify network configurations and settings.
Software Discovery: Security Software Discovery	<u>T1518.001</u>	Play ransomware actors scan for anti-virus software.

*Table 5: Play ATT&CK Techniques for Enterprise for Defense Evasion*

Technique Title	ID	Use
Impair Defenses: Disable or Modify Tools	<u>T1562.001</u>	Play ransomware actors use tools like GMER, IOBit, and PowerTool to disable anti-virus software.
Indicator Removal: Clear Windows Event Logs	<u>T1070.001</u>	Play ransomware actors delete logs or other indicators of compromise to hide intrusion activity.

**TLP:CLEAR**

JOINT  
**CYBERSECURITY ADVISORY**

TLP:CLEAR

FBI | CISA | ACSC

Table 6: Play ATT&amp;CK Techniques for Enterprise for Credential Access

Technique Title	ID	Use
Unsecured Credentials	<u>T1552</u>	Play ransomware actors attempt to identify and exploit credentials stored unsecurely on a compromised network.
OS Credential Dumping	<u>T1003</u>	Play ransomware actors use tools like Mimikatz to dump credentials.

Table 7: Play ATT&amp;CK Techniques for Enterprise for Lateral Movement

Technique Title	ID	Use
Lateral Tool Transfer	<u>T1570</u>	Play ransomware actors distribute executables within the compromised environment.

Table 8: Play ATT&amp;CK Techniques for Enterprise for Command and Control

Technique Title	ID	Use
Domain Policy Modification: Group Policy Modification	<u>T1484.001</u>	Play ransomware actors distribute executables via Group Policy Objects.

Table 9: Play ATT&amp;CK Techniques for Enterprise for Collection

Technique Title	ID	Use
Archive Collected Data: Archive via Utility	<u>T1560.001</u>	Play ransomware actors use tools like WinRAR to compress files.

Table 10: Play ATT&amp;CK Techniques for Enterprise for Exfiltration

Technique Title	ID	Use
Exfiltration Over Alternative Protocol	<u>T1048</u>	Play ransomware actors use file transfer tools like WinSCP to transfer data.

Table 11: Play ATT&amp;CK Techniques for Enterprise for Impact

Technique Title	ID	Use
Data Encrypted for Impact	<u>T1486</u>	Play ransomware actors encrypt data on target systems to interrupt availability to system and network resources.
Financial Theft	<u>T1657</u>	Play ransomware actors use a double-extortion model for financial gain.

TLP:CLEAR



JOINT

# CYBERSECURITY ADVISORY



FBI | CISA | ACSC

**TLP: CLEAR**

## MITIGATIONS

The FBI, CISA, and ASD's ACSC recommend organizations apply the following mitigations to limit potential adversarial use of common system and network discovery techniques and to reduce the risk of compromise by Play ransomware. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats and TTPs. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

These mitigations apply to all critical infrastructure organizations and network defenders. The FBI, CISA, and ASD's ACSC recommend that software manufacturers incorporate secure-by-design and -default principles and tactics into their software development practices to limit the impact of ransomware techniques (such as threat actors leveraging backdoor vulnerabilities into remote software systems), thus, strengthening the security posture for their customers.

For more information on secure by design, see CISA's Secure by Design and Default webpage and joint guide.

- **Implement a recovery plan** to maintain and retain multiple copies of sensitive or proprietary data and servers [CPG 2.F, 2.R, 2.S] in a physically separate, segmented, and secure location (i.e., hard drive, storage device, the cloud).
- **Require all accounts** with password logins (e.g., service account, admin accounts, and domain admin accounts) to **comply** with NIST's standards for developing and managing password policies [CPG 2.C].
  - Use longer passwords consisting of at least 8 characters and no more than 64 characters in length [CPG 2.B];
  - Store passwords in hashed format using industry-recognized password managers;
  - Add password user "salts" to shared login credentials;
  - Avoid reusing passwords;
  - Implement multiple failed login attempt account lockouts [CPG 2.G];
  - Disable password "hints";
  - Refrain from requiring password changes more frequently than once per year.

**Note:** NIST guidance suggests favoring longer passwords instead of requiring regular and frequent password resets. Frequent password resets are more likely to result in users developing password "patterns" cyber criminals can easily decipher.

  - Require administrator credentials to install software.
- **Require multifactor authentication** [CPG 2.H] for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems. Also see Protect Yourself: Multi-Factor Authentication | Cyber.gov.au.
- **Keep all operating systems, software, and firmware up to date.** Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Prioritize patching known exploited vulnerabilities in internet-facing

**TLP: CLEAR**

JOINT  
**CYBERSECURITY ADVISORY**

FBI | CISA | ACSC

**TLP:CLEAR**

systems [CPG 1.E]. Organizations are advised to deploy the latest Microsoft Exchange security updates. If unable to patch, then disable Outlook Web Access (OWA) until updates are able to be undertaken. Also see Patching Applications and Operating Systems | Cyber.gov.au.

- **Segment networks** [CPG 2.F] to prevent the spread of ransomware. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks and by restricting adversary lateral movement. Also see Implementing Network Segmentation and Segregation.
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware** with a networking monitoring tool. To aid in detecting the ransomware, implement a tool that logs and reports all network traffic, including lateral movement activity on a network [CPG 1.E]. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.
- **Filter network traffic** by preventing unknown or untrusted origins from accessing remote services on internal systems. This prevents actors from directly connecting to remote access services they have established for persistence. Also see Inbound Traffic Filtering – Technique D3-ITF.
- **Install, regularly update, and enable real time detection for antivirus software** on all hosts.
- **Review domain controllers, servers, workstations, and active directories** for new and/or unrecognized accounts [CPG 1.A, 2.O].
- **Audit user accounts** with administrative privileges and configure access controls according to the principle of least privilege [CPG 2.E].
- **Disable unused ports** [CPG 2.V].
- **Consider adding an email banner to emails** [CPG 2.M] received from outside your organization.
- **Disable hyperlinks** in received emails.
- **Implement time-based access for accounts set at the admin level and higher.** For example, the just-in-time (JIT) access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the Zero Trust model). This is a process where a network-wide policy is set in place to automatically disable admin accounts at the Active Directory level when the account is not in direct need. Individual users may submit their requests through an automated process that grants them access to a specified system for a set timeframe when they need to support the completion of a certain task.
- **Disable command-line and scripting activities and permissions.** Privileged escalation and lateral movement often depend on software utilities running from the command line. If threat actors are not able to run these tools, they will have difficulty escalating privileges and/or moving laterally [CPG 2.E].

**TLP:CLEAR**

# JOINT CYBERSECURITY ADVISORY

**TLP:CLEAR**

FBI | CISA | ACSC

- **Maintain offline backups of data** and regularly maintain backup and restoration [CPG 2.R]. By instituting this practice, an organization ensures they will not be severely interrupted, and/or only have irretrievable data.
- **Ensure backup data is encrypted, immutable** (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure [CPG 2.K].

## VALIDATE SECURITY CONTROLS

In addition to applying mitigations, the FBI, CISA, and ASD's ACSC recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. The FBI, CISA, and ASD's ACSC recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see Tables 3-11).
2. Align your security technologies against this technique.
3. Test your technologies against this technique.
4. Analyze your detection and prevention technologies performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

The FBI, CISA, and ASD's ACSC recommend continually testing your security program at scale and in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

## RESOURCES

- [Stopransomware.gov](https://stopransomware.gov) is a whole-of-government approach that gives one central location for ransomware resources and alerts.
- Resource to mitigate a ransomware attack: [#StopRansomware Guide](#).
- No-cost cyber hygiene services: [Cyber Hygiene Services](#) and [Ransomware Readiness Assessment](#).

## REPORTING

The FBI is seeking any information that can be shared, to include boundary logs showing communication to and from foreign IP addresses, a sample ransom note, communications with Play ransomware actors, Bitcoin wallet information, decryptor files, and/or a benign sample of an encrypted file.

The FBI, CISA, and ASD's ACSC do not encourage paying ransom as payment does not guarantee victim files will be recovered. Furthermore, payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware,

**TLP:CLEAR**

**JOINT  
CYBERSECURITY ADVISORY****TLP:CLEAR**

FBI | CISA | ACSC

and/or fund illicit activities. Regardless of whether you or your organization have decided to pay the ransom, the FBI and CISA urge you to promptly report ransomware incidents to a local FBI Field Office, the FBI's Internet Crime Complaint Center (IC3), or CISA via CISA's 24/7 Operations Center (report@cisa.gov or 888-282-0870).

Australian organizations that have been impacted or require assistance in regard to a ransomware incident can contact ASD's ACSC via 1300 CYBER1 (1300 292 371), or by submitting a report to cyber.gov.au.

**DISCLAIMER**

The information in this report is being provided "as is" for informational purposes only. CISA and the FBI do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA or the FBI.

**REFERENCES**

- [1] Symantec: Play Ransomware Group Using New Custom Data-Gathering Tools
- [2] TrendMicro: Play Ransomware Spotlight
- [3] SentinelLabs: Ransomware Developers Turn to Intermittent Encryption to Evade Detection

**TLP:CLEAR**

# ***EXHIBIT 6***

BRANDON M. DALZIEL  
BDALZIEL@BODMANLAW.COM  
313-393-7507

December 19, 2024

*Via Certified Mail*

BODMAN PLC  
6TH FLOOR AT FORD FIELD  
1901 ST. ANTOINE STREET  
DETROIT, MICHIGAN 48226  
313-393-7579 FAX  
313-259-7777

Change Healthcare  
P. O. Box 742526  
Atlanta, GA 30374-2526 USA

Re: **Demand for Resolution to Ongoing Issues and Information to  
Calculate Damages Caused by Change Healthcare Breach**

Dear Sir or Madam:

**bodman**  
ATTORNEYS & COUNSELORS

This firm represents Basha Diagnostics, P.C. ("Basha"). This letter is in follow-up to many ongoing complications and repercussions caused as a result of Change Healthcare's February 21, 2024, cyber incident and failure of representatives of Change Healthcare to provide substantive or acceptable guidance, replies or commitments.

This letter constitutes additional written notice of Change Healthcare's continuous breach of its material duties and obligations under the Master Services Agreement between Change Healthcare and Basha Diagnostics, P.C. (the "Agreement"). This letter also constitutes additional written notice of Change Healthcare's failure to perform its material duties or obligations under the Agreement, including Section 2.2.1 of Schedule 1 and Section 2.2.1 of Schedule 2 (previously notices have been provided, including by Basha on March 8, 2024). For example, (a) Schedule 1, 2.2.1(c): Change Healthcare will, "prepare and submit claims to insurance carriers or to patients directly if no insurance information was provided within twenty four (24) hours of receipt of all information necessary to submit the claims;" and (b) Schedule 2, 2.1.1.(a)(i): Change Healthcare will, "Provide 24 hour access, less scheduled or unscheduled downtime for-maintenance or repair, from any Internet access point to the Client reporting portal."

In short, Basha wholly depended on Change Healthcare for critical functions of its operations and Change Healthcare failed to provide its required services. Due to Change Healthcare and its breaches, Basha had been unable to initiate, process, or receive proceeds of insurance claims from its patients and their insurers.

In addition to Change Healthcare's failure to prevent the cyber event, Change Healthcare also failed to properly respond to it. Among other failures, Change Healthcare failed to notify Basha of the intrusion in a timely manner and failed to quickly restore services. In that regard, Change Healthcare's client-facing response to the incident was wholly inadequate. For example, rather than increase customer service and provide additional patient service representative resources, Change Healthcare appears to have done the opposite, leaving Basha to address Change

DETROIT | TROY | ANN ARBOR | GRAND RAPIDS

December 19, 2024  
Page 2

Healthcare's catastrophic failures and to be the sole means for patients to ask questions, demand answers, voice frustrations, etc.

At this point, it appears that Basha's losses could be in excess of \$8,000,000. This amount is comprised of lost revenue caused by the rejection of claims to patient insurers due to Change Healthcare's failures, and does not even include other damages such additional costs for additional personnel and time spent in an effort to complete the services that were Change Healthcare's obligations in an effort to mitigate harm to Basha's business.

Change Healthcare has effectively failed to provide any customer support in the wake of this incident. Our patients have attempted to reach customer service representatives on numerous occasions with limited or no response. Basha has many specific examples of notable issues, including accounts of Optum representatives being rude and potentially hanging up on patients. Such interactions cause damage to Basha, and Basha is left receiving complaints that are ultimately due to Change Healthcare, as well as using resources to mitigate such reputational and other damages.

Additionally, Change Healthcare's software has repeatedly sent incorrect statements to patients that indicate such patients have an outstanding balance when no such balance is due. Basha has numerous accounts of such issues together with patients then attempting to follow-up with Optum, only to be left on hold for several hours and/or having called Optum multiple days in row without receiving a response.

Basha wholly depends on Change Healthcare for critical functions of its operations and Change Healthcare has failed to provide its contractually-required services. It is imperative that Change Healthcare promptly provide resolutions to each of the above issues so that Basha can resume normal operations.

In addition to the ongoing catastrophic operational complications, as a result of Change Healthcare's breach Basha has been forced to file a claim with its insurance provider. The claim process has been challenging for many reasons, including due to the significant delay and issues involving Change Healthcare services, which has resulted in the amount of the damage caused by the breach remaining unclear. Basha demands that Change Healthcare provide by December 31, 2024, the following information which is being required by the insurance company:

1. Monthly Billing & Collections reports for February 2024 through the most recent available.
2. Monthly Profit & Loss Statements, by individual month, for January 2023 through September 2024
3. Report detailing patient charges generated, which could not billed, from January and February 2024



December 19, 2024

Page 3

4. Report detailing, on a monthly basis: data clearly showing claims lost, rejected, out of time windows, not billed, and/or not collectible, from January 2023 through November 2024 .
5. Copy of Loan Agreement/Line of Credit Application

Nothing contained herein shall constitute or should be construed to constitute a waiver of rights, claims or defenses on the part of Basha, and all such rights, claims and defenses are expressly reserved, including as a result of defaults under the Agreement and applicable law, including without limitation the right to potentially terminate the Agreement immediately, including due to Change Healthcare's inability to cure. Basha reserves all rights and remedies.


Please contact me immediately to discuss.


Sincerely,



Brandon M. Dalziel

c: Yahya Mossa Basha, M.D., Basha Diagnostics, P.C. ([bashadiagnostics@aol.com](mailto:bashadiagnostics@aol.com))  
Feras Basha, M.D., Basha Diagnostics, P.C. ([fmbasha@gmail.com](mailto:fmbasha@gmail.com))  
Jasmina Jakupovic, Basha Diagnostics, P.C. ([jasmina@bashaopenmri.com](mailto:jasmina@bashaopenmri.com))  
Roger Connor ([roger.connor@optum.com](mailto:roger.connor@optum.com))  
Michael Summers ([michael.summers1@optum.com](mailto:michael.summers1@optum.com))  
Christine J. Muraski ([christine.muraski@optum.com](mailto:christine.muraski@optum.com))  
Sarah D. King ([sarahking@optum.com](mailto:sarahking@optum.com))

SENDER: COMPLETE THIS SECTION		COMPLETE THIS SECTION ON DELIVERY	
<p>■ Complete items 1, 2, and 3.</p> <p>■ Print your name and address on the reverse so that we can return the card to you.</p> <p>■ Attach this card to the back of the mailpiece, or on the front if space permits.</p>		<p>A. Signature <b>X</b> <span style="float: right;"><input type="checkbox"/> Agent <input type="checkbox"/> Addressee</span></p>	
<p>1. Article Addressed to:</p> <p style="text-align: center;">Change Healthcare P. O. Box 742526 Atlanta, GA 30374-2526 USA</p>  <p style="text-align: center;">9590 9402 8430 3156 2289 85</p>		<p>B. Received by (Printed Name) _____ C. Date of Delivery _____</p>	
<p>2. Article Number (Transfer from service label)</p> <p style="text-align: center;">9589 0710 5270 2130 6544 33</p>		<p>D. Is delivery address different from item 1? <input type="checkbox"/> Yes If YES, enter delivery address below: <input type="checkbox"/> No</p>	
		<p>3. Service Type <span style="float: right;"><input type="checkbox"/> Priority Mail Express®</span></p> <p><input type="checkbox"/> Adult Signature <span style="float: right;"><input type="checkbox"/> Registered Mail™</span></p> <p><input type="checkbox"/> Adult Signature Restricted Delivery <span style="float: right;"><input type="checkbox"/> Registered Mail Restricted Delivery</span></p> <p><input type="checkbox"/> Certified Mail® <span style="float: right;"><input type="checkbox"/> Signature Confirmation™</span></p> <p><input type="checkbox"/> Certified Mail Restricted Delivery <span style="float: right;"><input type="checkbox"/> Signature Confirmation Restricted Delivery</span></p> <p><input type="checkbox"/> Collect on Delivery <span style="float: right;"><input type="checkbox"/> Signature Confirmation Restricted Delivery</span></p> <p><input type="checkbox"/> Collect on Delivery Restricted Delivery <span style="float: right;"><input type="checkbox"/> Signature Confirmation Restricted Delivery</span></p> <p><input type="checkbox"/> Insured Mail <span style="float: right;"><input type="checkbox"/> Signature Confirmation Restricted Delivery</span></p> <p><input type="checkbox"/> Insured Mail Restricted Delivery</p>	
PS Form 3811, July 2020 PSN 7530-02-000-9053		Domestic Return Receipt	

U.S. Postal Service™ CERTIFIED MAIL® RECEIPT Domestic Mail Only	
For delivery information, visit our website at <a href="http://www.usps.com">www.usps.com</a> ®.	
<p>Certified Mail Fee \$ _____</p> <p>Extra Services &amp; Fees (check box, add fee as appropriate)</p> <p><input type="checkbox"/> Return Receipt (hardcopy) \$ _____</p> <p><input type="checkbox"/> Return Receipt (electronic) \$ _____</p> <p><input type="checkbox"/> Certified Mail Restricted Delivery \$ _____</p> <p><input type="checkbox"/> Adult Signature Required \$ _____</p> <p><input type="checkbox"/> Adult Signature Restricted Delivery \$ _____</p> <p>Postage \$ _____</p> <p>Total Postage and Fees \$ _____</p> <p>Sent To _____</p> <p>Street and Apt. No. _____</p> <p>City, State, ZIP+4® _____</p>	
<p>PLACE STICKER AT TOP OF ENVELOPE TO THE RIGHT OF THE RETURN ADDRESS. FOLD AT DOTTED LINE</p> <p><b>CERTIFIED MAIL®</b></p>  <p>9589 0710 5270 2130 6544 33</p> <p>9589 0710 5270 2130 6544 33</p>	<p>Postmark Here</p> <p style="text-align: center;">Change Healthcare P. O. Box 742526 Atlanta, GA 30374-2526 USA</p>
PS Form 3800, January 2023 PSN 7530-02-000-9047 See Reverse for Instructions	

Original – Court

**STATE OF MICHIGAN  
6<sup>TH</sup> JUDICIAL CIRCUIT  
COUNTY OF OAKLAND****NOTICE OF ASSIGNMENT TO THE  
BUSINESS COURT****CASE NO.**  
**2025-212987-CB**  
**JUDGE VICTORIA****Court address**  
1200 N Telegraph Rd Pontiac, MI 48341**VALENTINE****Court telephone no.**  
248-858-0345**Plaintiff's name(s), address(es), and telephone number(s)**  
BASHA DIAGNOSTICS, P.C.**Plaintiff's attorney, bar no., address, telephone no., and email address**  
Michelle Thurber Czapski (P47267) | Erica J. Sarver (P80106) |  
Nashara A.L. Peart (P83078)  
201 W. Big Beaver Road, Suite 500, Troy, Michigan 48084  
(248) 743-6000  
mzczapski@bodmanlaw.com | esarver@bodmanlaw.com  
npeart@bodmanlaw.com

v

**Defendant's name(s), address(es), and telephone number(s)**  
CHANGE HEALTHCARE TECHNOLOGY ENABLED  
SERVICES, LLC, CHANGE HEALTHCARE, INC.,  
OPTUM INC., UNITEDHEALTH GROUP, INC., and  
UNITEDHEALTHCARE, INC.**Defendant's attorney, bar no., address, telephone no., and email address**  
This case has been designated as an eFiling case,  
for more information please visit  
[www.oakgov.com/efiling](http://www.oakgov.com/efiling).

The ☒ Plaintiff ☐ Defendant requests assignment of the above captioned matter to the Business Court. The case qualifies for the Business Court and the matter should be identified as Business Court eligible pursuant to MCL 600.8031, MCL 600.8035, and LAO 2024-01 as indicated below. (Check all that apply.)

The case qualifies as business or commercial dispute as defined by MCR 2.112(O) and MCL 600.8031(1)(c)(i)-(iii) as:

- ☒ All of the parties are business enterprises;
- ☐ One or more of the parties is a business enterprise and the other parties are its or their present or former owners, managers, shareholders, members of a limited liability company or similar business organization, directors, officers, agents, employees, suppliers, guarantors of a commercial loan, or competitors, and the claims arise out of those relationships;
- ☐ One of the parties is a nonprofit organization and the claims arise out of that party's organizational structure, governance, or finances.

Pursuant to MCL 600.8031(2) the business or commercial dispute includes, but is not limited to, those involving:

- ☐ The sale, merger, purchase, combination, dissolution, liquidation, organizational structure, governance, or finance of a business enterprise;
- ☒ Information technology, software, or website development, maintenance or hosting;
- ☐ The internal organization of business entities and the rights or obligations of shareholders, partners, members, owners, officers, directors, or managers;
- ☒ Contractual agreements or other business dealings, including licensing, trade secret, intellectual property, antitrust, securities, noncompete, nonsolicitation, and confidentiality agreements if all available administrative remedies are completely exhausted, including, but not limited to, alternative dispute resolution processes prescribed in the agreements;
- ☐ Commercial transactions, including commercial bank transactions;
- ☐ Business or commercial insurance policies; and/or
- ☐ Commercial real property.
- ☐ Other: (Please explain)

February 20, 2025

Date

Michelle Thurber Czapski (P47267)

Name

Attorney for: Plaintiff